LP-3014PW Wireless ADSL Modem

Installation Guide

and

User's Manual

Version 2.0.16

COMTAC.

© Copyright 2002-2004 COMTAC. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, decryption, decompilation, and reverse engineering. No part of this product or document may be reproduced in any form by any means without prior written authorization of COMTAC. or its licensors, if any.

The information in this document is subject to change without notice. This documentation is provided “as is” and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaims are held to be legally invalid.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION TO WIRELESS ADSL MODEM ROUTER 1

PRODUCT FEATURES 1
RELATED DOCUMENTS 4

CHAPTER 2 BEFORE INSTALLATION 5

PACKAGE CONTENT 5
HARDWARE INDICATORS 5
Front Panel 5
Wireless ADSL Ethernet Modem Router (Single-Port) 5
Wireless ADSL Ethernet Modem Router (Four-Ports) 6
Rear Panel 6
Wireless ADSL Ethernet Modem Router (Single-Port) 6
Wireless ADSL Ethernet Modem Router (Four-Port) 7

CHAPTER 3 HARDWARE INSTALLATION 8

LP-AL3011PW 8
LP-AL3014PW 9
INSTALLATION PROCEDURES 10

CHAPTER 4 NETWORKING SETTINGS 11

TCP/IP CONFIGURATION FOR WINDOWS 95/98/ME 11
TCP/IP CONFIGURATION FOR WINDOWS W2K/XP 15
CHECK YOUR TCP/IP PROTOCOL 18

CHAPTER 5 ACCESS AND STATUS OF MODEM 19

ACCESSING THE WEB MANAGER 19
MODEM STATUS 19
Home Page 20
PPP Page 20
ADSL Status Page 21

CHAPTER 6 CONFIGURE ADSL MODEM 22

WAN CONFIGURATION 22
PPPoE / PPPoA mode with DHCP function 23
Router mode for Static IP with DHCP function 24
Bridge mode with DHCP function 25
Additional Configuration of Router Modes 26
Dynamic IP for WAN IP 26
Static IP for WAN IP 26
PPPoA (RFC 2364) 26
PPPoE (RFC 2516) 27
Classical IP over ATM (RFC 1577) 27
Per VC Settings 28
Bridge Mode 28
IGMP 29
ATM 30
DHCP Client 32
MAC Spoofing 32
Static IP Settings 32
PPP Configuration 33
LAN CONFIGURATION 34
PPP CONFIGURATION 36

PPP DISCONNECT TIMER CONFIGURATION 38
Enable/Disable Idle Timer Filter *38*
Filter Application *38*
Filter Details *39*
NAT CONFIGURATION 41
NAT (Static) *41*
NAPT (Static) *42*
VIRTUAL SERVER 43
BRIDGE FILTERING 45
DNS CONFIGURATION 46
WIRELESS 48
WIRELESS LAN (WLAN) SECURITY 50
USER LEVEL USERNAME/PASSWORD 51
SAVE SETTINGS / REBOOT 52

CHAPTER 7 ADMIN PRIVILEGE 53

WAN STATUS 53
ATM STATUS 53
ADSL CONFIGURATION 54
ROUTE TABLE 55
System Default Gateway Configuration *56*
Route Configuration *57*
LEARNED MAC TABLE 57
RIP CONFIGURATION 58
RIP Per Interface Configuration *60*
SNMP CONFIGURATION 62
MISCELLANEOUS CONFIGURATION 64
TCP STATUS 68
ADMIN PASSWORD CONFIGURATION 69
RESET TO FACTORY DEFAULT 70
DIAGNOSTIC TEST 71
SYSTEM LOG 74
LOCAL CODE IMAGE UPDATE 75

CHAPTER 8 FIREWALL CONFIGURATION 76

PROTECTION POLICY 77
HACKER LOG 79
SERVICE FILTERING 80
IP GROUP 81
SERVICE GROUP 83
TIME WINDOW 84
INBOUND POLICY 85
OUTBOUND POLICY 89
INBOUND/OUTBOUND POLICY SAMPLE CONFIGURATION 93
Inbound Policy *93*
Outbound Policy *94*

APPENDIX A: ADSL ETHERNET MODEM ROUTER CONFIGURATION 96

BRIDGE MODE CONFIGURATION 96
ROUTER MODE CONFIGURATION WITH DYNAMIC IP 97
ROUTER MODE CONFIGURATION WITH STATIC IP 98
ROUTER MODE PPPOA CONFIGURATION (RFC2364) 99
ROUTER MODE PPPOE CONFIGURATION (RFC2516) 100
ROUTER MODE CONFIGURATION WITH CLASSICAL IP OVER ATM (RFC1577) 101

CHAPTER 1

INTRODUCTION TO WIRELESS ADSL MODEM ROUTER

The Wireless ADSL Ethernet Modem Router is optimized to address the growing demand for high-speed Internet access. With an USB 1.1-compliant interface, an IEEE 802.3-compliant Ethernet interface and a high performance 54Mbps IEEE 802.11g compliant interface, this complete device provides the widest array of connectivity options without relaying on host PC drivers.

The Wireless ADSL Ethernet Modem Router provides an "always-on" high-speed broadband connection to the internet. Using existing twisted-pair telephone lines, ADSL technology provides data rates more than 100 times as fast as a traditional analog modem, without an interruption in telephone service.

This Wireless ADSL Ethernet Modem Router is fully compliant with the full-rate ADSL(T1.413 Issue 2 and G.dmt), the splitterless G.lite (G.992.2) and IEEE 802.11g standards. With data transfer rates of up to 8 Mbps downstream and 1Mbps upstream for ADSL transmission

Product Features

- ADSL Compliance
  - Compliant with ADSL standards
    - ✓ Full-rate ANSI T1.413 Issue 2 and ITU G.dmt (G.992.1) standards
    - ✓ Splitterless ITU G.lite (G.992.2) specification
    - ✓ ADSL over POTS (Annex A) and ADSL over ISDN (Annex B)
  - DMT modulation and demodulation
  - Full-rate adaptive modem
    - ✓ Maximum downstream rate of 8 Mbps
    - ✓ Maximum upstream rate of 1 Mbps
  - Tone detection for low power mode
  - Supports splitterless ADSL implementation
  - Supports Dying Gasp (Option)

- **ATM Protocols**
  - WAN mode support: PPP over ATM (RFC 2364) and PPP over Ethernet (RFC2516)
  - LAN mode support: bridged/routed Ethernet over ATM (RFC 1483) and Classical IP over ATM (RFC 1577)

- ATM Forum UNI 3.1/4.0 PVC
- Up to 8 VCs (Virtual Circuits)
- ATM SAR (Segmentation and Reassembly)
- ATM AAL5 (Adoption Layer type 5)
- OAM F4/F5

- **Bridge Mode**
  - Ethernet to ADSL self-learning Transparent Bridging (IEEE 802.1D)
  - Supports up to 128 MAC learning addresses Router Mode

- **Router Mode**
  - IP routing – RIPv2 (Backward compatible with RIPv1)
  - Static routing
  - DHCP (Dynamic Host Configuration Protocol) Server and Client
  - NAPT (Network Address and Port Translation)
  - NAT (Network Address Translation)
  - ICMP (Internet Control Message Protocol
  - Simultaneous USB and Ethernet operation
  - IGMP (Internet Group Management Protocol)

- **Security**
  - User authentication for PPP
  - PAP (Password Authentication Protocol)\
  - CHAP (Challenge Authentication Protocol)
  - Password protected system management
  - RADIUS client authentication

- **USB Host Interface**
  - Compliant with USB Specification, Revision 1.1
  - USB full speed (12 Mbps)
  - Vendor specific descriptors

- **Wireless IEEE 802.11g Compliance**
  - 54Mbps Access Point for wireless connectivity
  - Interoperable with IEEE 802.11g(PBCC & OFDM Modulation Technology Supports) 2.4GHz compliance equipment
  - 128-bit and 64-bit WEP support
  - WPA support

- **HTTP Web-based Management**
  - Firmware upgrade via FTP
  - Customizable Web pages
  - WAN and LAN side connection statistics
  - Configuration of static routes and Routing table
  - Configuration of NAT/NAPT
  - Password protected access
  - Selection of Bridge or Router Mode
  - PPP user ID and password
  - Configuration of VCs (Virtual Circuits)

- **Ethernet Interface**
  - IEEE 802.3 compliant
  - 10/100 Mbps
  - Simultaneous operation with USB

- **ADSL Ethernet Modem Router (Four-Port Only)**
  - Each port can work at 10 Mbps or 100Mbps, full-duplex or half-duplex mode
  - Automatic MDI/MDIX crossover for 100Base-TX and 10Base-T ports
  - Auto-negotiation and speed-auto-sensing support
  - Back-pressure-based flow control on half-duplex ports
  - Pause-frame-based flow control on full duplex ports
  - Store-and-forward switching mode
  - High performance lookup engine with support for up to 4096 MAC address entries with automatic learning and aging

- **Password protection access (2 levels)**
  - Selection of bridge or router mode
  - PPP user ID and password
  - Configuration of VCs (Virtual circuits)
  - System Logging
  - Restore to Factory defaults via Web or Hardware
  - FTP server and client

Related Documents

- ITU G.992.1 (G.dmt *Full-rate ADSL*)
- ITU.G.992.2 (G.lite "*Splitterless ADSL"*)
- RFC 768 User Datagram Protocol (UDP)
- RFC 791 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 Transmission Control Protocol (TCP)
- RFC 826 Ethernet Address Resolution Protocol (ARP)
- RFC 1334 Password Authentication Protocol (PAP)
- RFC 1483 Multi-protocol Encapsulation over ATM
- RFC 1552 Point-to-Point Protocol (PPP)
- RFC 1577 Classical IP and ARP over ATM
- RFC 1631 Network Address Translation (NAT)
- RFC 1638 Bridge Control Protocol (BCP) for the Point-to-Point Protocol(PPP)
- RFC 1661 Link Control Protocol (LCP) for the Point-to-Point Protocol(PPP)
- RFC 1723 Routing Information Protocol Version 2
- RFC 1994 Challenged Handshake Authentication Protocol (CHAP)
- RFC 2131 Dynamic Host Configuration Protocol
- RFC 2364 PPP over ATM
- RFC 2516 PPP over Ethernet
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.1d
- IEEE 802.11g

CHAPTER 2 BEFORE INSTALLATION

Package Content

Make sure that you have the following items:

- ADSL Wireless Ethernet Modem Router (Single-Port/Four-Ports)
- 12VDC Power Adaptor
- Telephone cable
- Installation guide
- Splitter/ CAT-5 UTP Fast Ethernet cable/ USB cable (Optional)

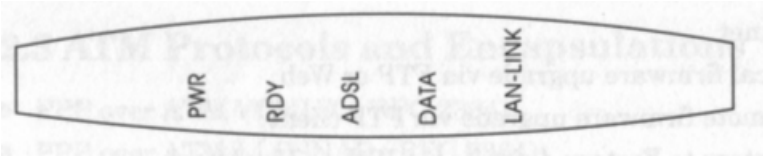
Note : If any of the items is damaged or missing, contact your dealer immediately.

Hardware Indicators

Front Panel

Place the Wireless ADSL Router in a location that permits an easy view of the LED indicators shown in the front panel diagram below.

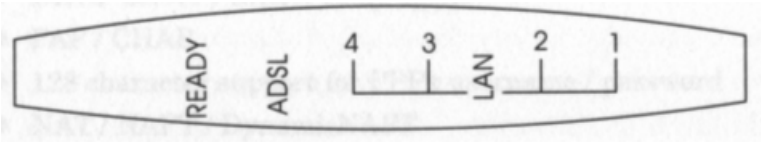
Wireless ADSL Ethernet Modem Router (Single-Port)



LED Indicators
The LED Indicators read as follows:

LED NAME	Descriptions
PWR	On: ADSL modem is power on
RDY	Blink: ADSL modem is ready Off: ADSL modem is not ready or has malfunctioned.
ADSL	Blink: ADSL modem is ready to connect or the link is down On: the ADSL modem links to DSLAM successfully.
DATA	Blink: when data is sent or received..
LAN-LINK	On: ADSL modem has a successful Ethernet connection.

Wireless ADSL Ethernet Modem Router (Four-Ports)



LED Indicators

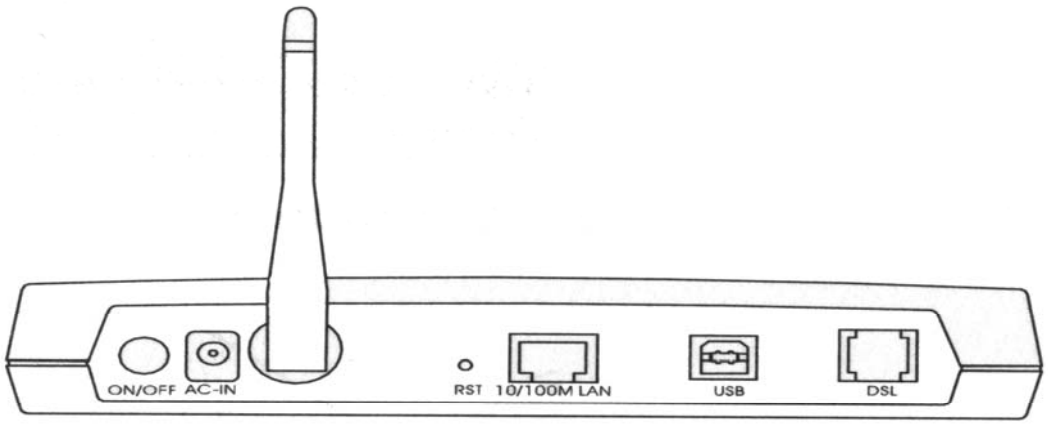
The LED Indicators read as follows:

LED NAME	Descriptions
READY	Blink: ADSL modem is ready. Off: ADSL modem is not ready or has malfunctioned. Always On: Please send back for repair.
ADSL	Blink: ADSL modem is ready to connect or the link is down On: ADSL modem links to DSLAM successfully.
LAN 1-4	On: ADSL modem has a successful Ethernet connection.

Rear Panel

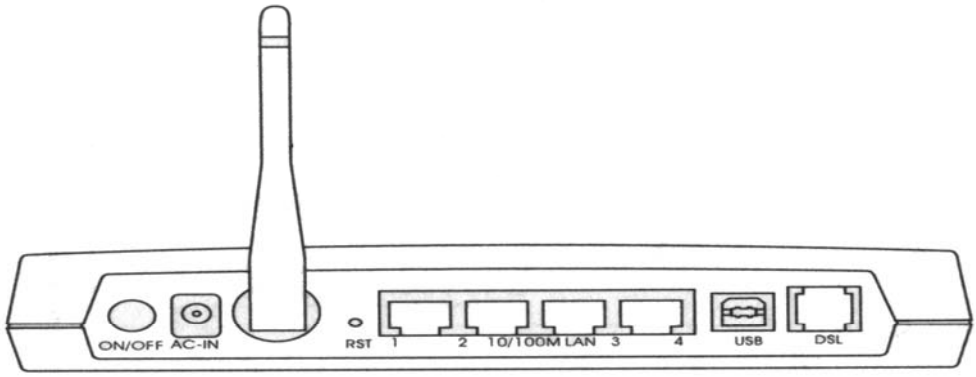
Wireless ADSL Ethernet Modem Router (Single-Port)

The rear panel of the Wireless Router provides access to the DC power adapter, one USB connection, one LAN connection, one WAN connection, one Antenna, and power on/off switch.



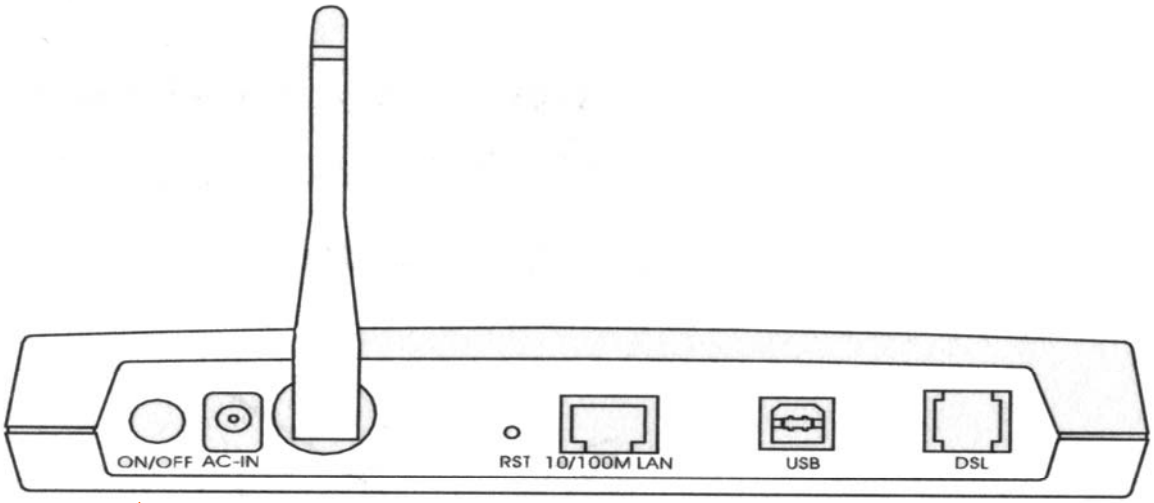
Wireless ADSL Ethernet Modem Router (Four-Port)

The rear panel of the Wireless Router provides access to the DC power adapter, one USB connection, four LAN connections, one WAN connection, one antenna, and power on/off switch.



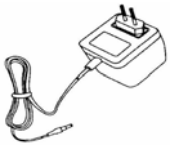
CHAPTER 3 HARDWARE INSTALLATION

LP-AL3011PW



Power Switch

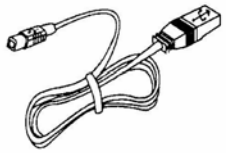
Power Adapter
Power cord connect here



Factory Reset button

RJ-45 Ethernet port connect
Ethernet cable here

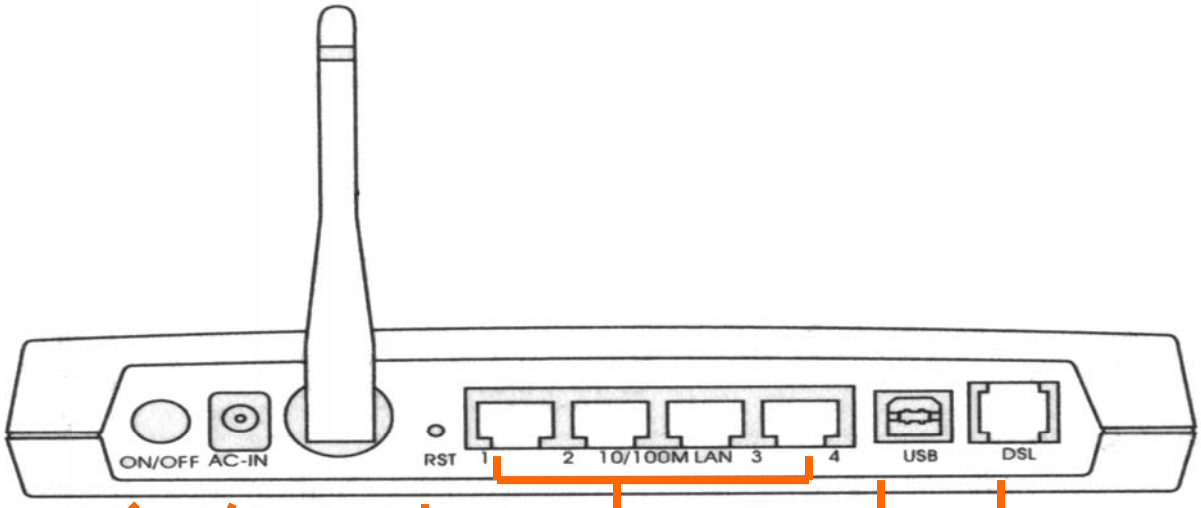
USB CABLE



Splitter (optional and changes depending on country specification)

RJ-11 ADSL port connect
ADSL cable here

LP-AL3014PW



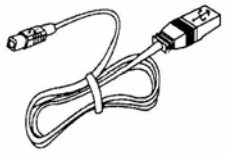
Power Switch

Factory Reset button

USB CABLE

Power Adapter
Power cord connect here

RJ-45 Ethernet port conn
Ethernet cable here



Splitter (optional and changes depending on country specification)

RJ-11 ADSL port connect
ADSL cable here

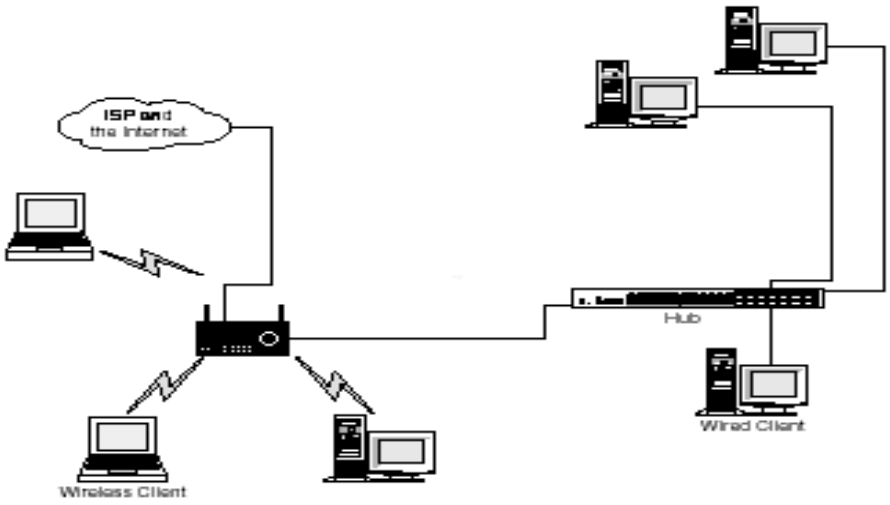
Installation Procedures

- Power on: Connect the Adapter to power inlet and turn the power switch on, this product will enter a self-test phase. When it is in the self-test phase, the indicators READY LED will be lighted ON for about 8 seconds, and the READY LED will be flashed to indicate that the self-test phase has finished. Finally, the READY LED will be flashed to indicate that router is in normal operation.

- ADSL connection: Simply plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into splitter.

- Connect Router to LAN: Prepare an Ethernet cable to connect Router to Hub or Switch of your LAN. You can connect Router to your PC directly by crossover Ethernet cable.

- LAN with Multiple Access Points, Wired Clients, and Wireless Clients:

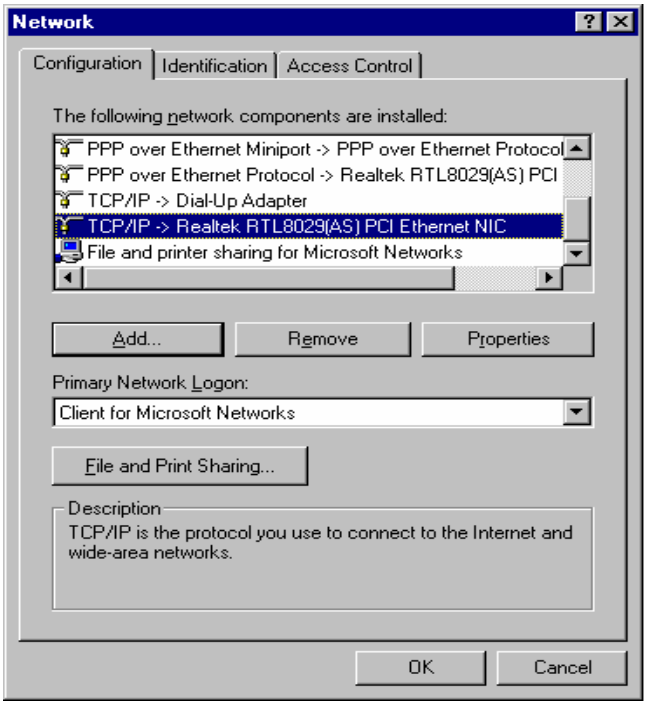


CHAPTER 4 NETWORKING SETTINGS

TCP/IP Configuration for Windows 95/98/ME

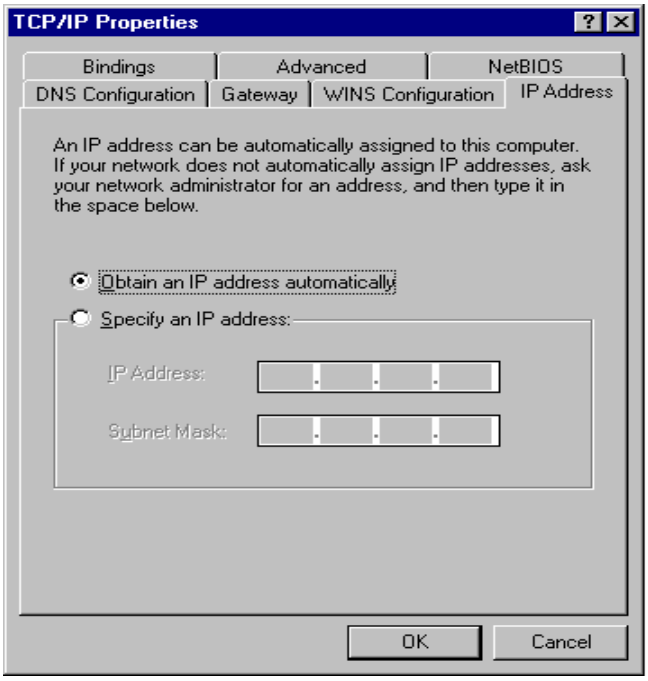
Use the following steps to configure the manager PC to be a DHCP client. These same steps must be performed for every host PC on your network if you use the DHCP function of the Router.

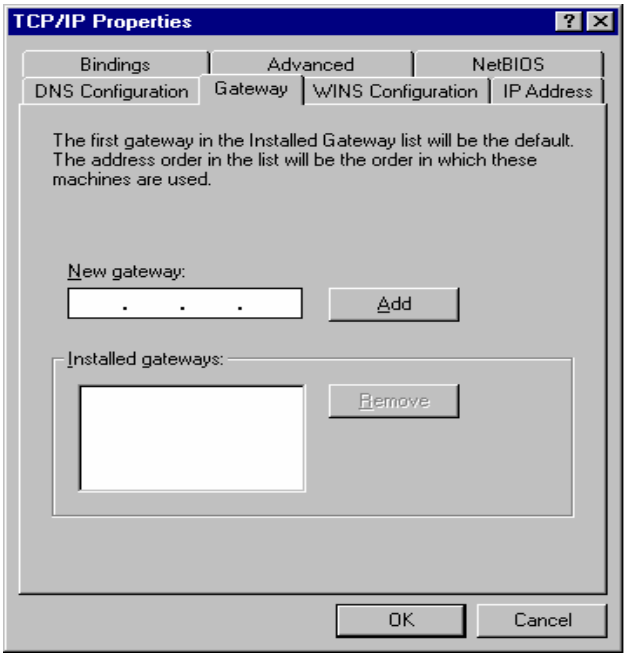
1. Click **Start** button, **Settings** and choose **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab.
3. Select the **TCP/IP** line that has been associated to your network card in the Configuration tab and click **Properties**.



4. Now, you have two setting methods:

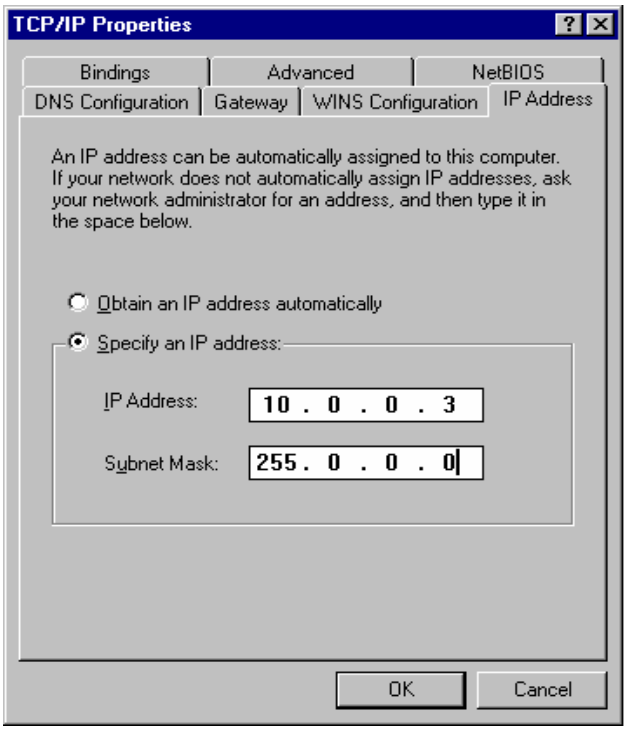
   A. Get IP Address from Router automatically (DHCP)


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

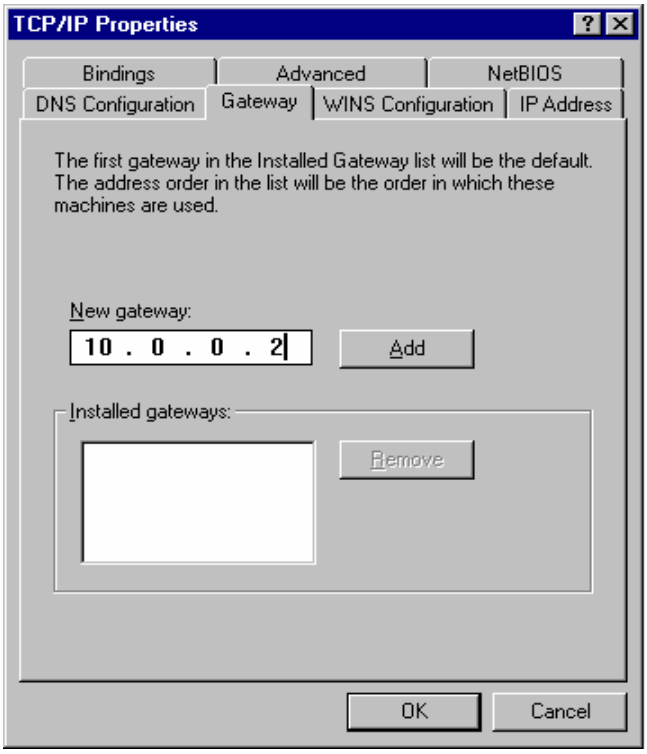


B. Configure IP Address manually.

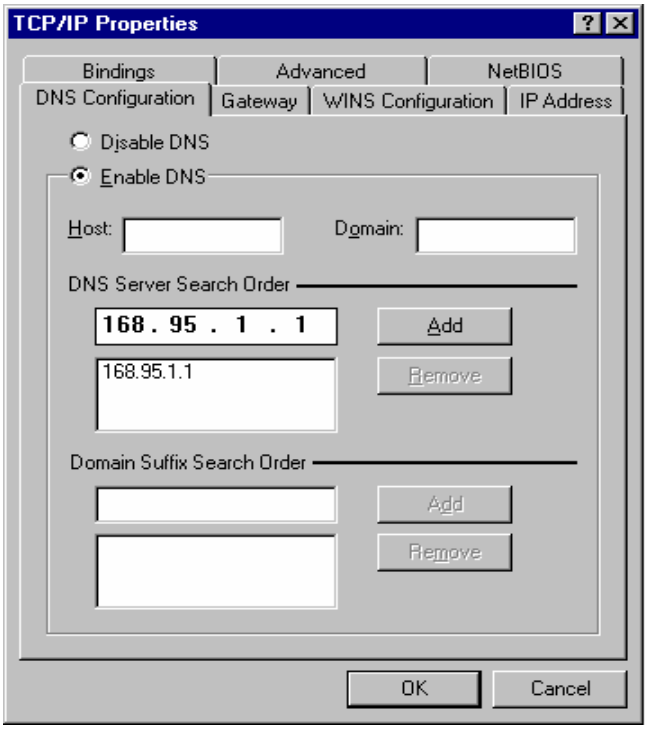
Select **Specify an IP address** on the *IP address tab*. The default IP address of Router is 10.0.0.2. So please use 10.0.0.X (X is between 1 and 253, except 2) for IP address field and 255.0.0.0.0 for *Subnet Mask* field.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
10 . 0 . 0 . 3
Subnet Mask:
255 . 0 . 0 . 0
OK
Cancel

In the *Gateway* tab, add the IP address of the Router (default IP is 10.0.0.2) in the New gateway field and click **Add** button.

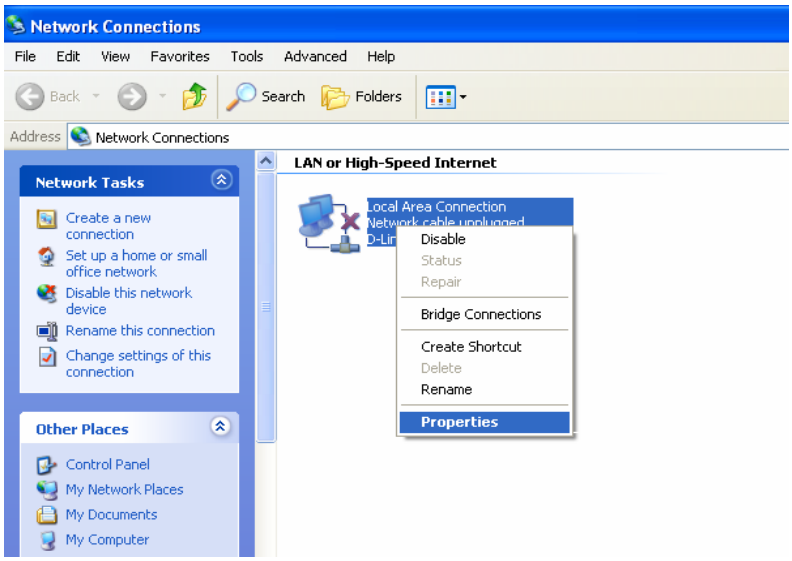


In the *DNS Configuration* tab, add the DNS values which are provided by the ISP into *DNS Server Search Order* field and click **Add** button.



TCP/IP Configuration for Windows W2K/XP

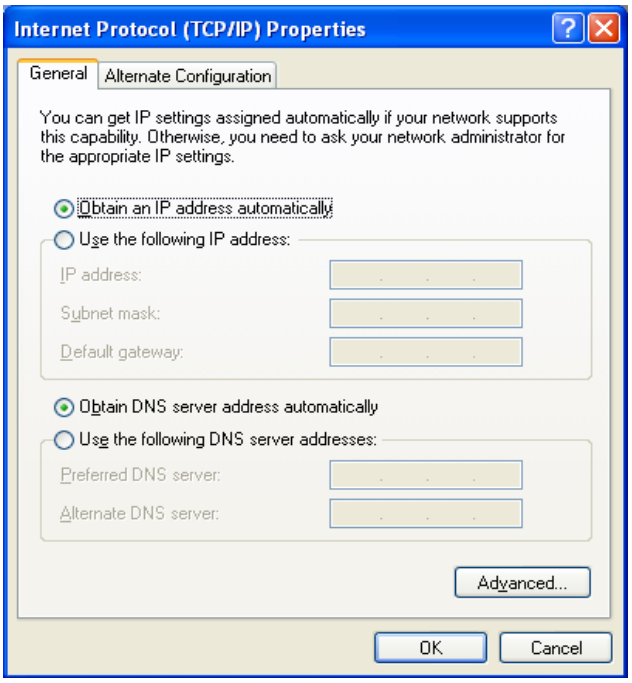
Use the following steps to configure the manager PC to be a DHCP client. These same steps must be performed for every host PC on your network if you use the DHCP function of the Router.



1. Click **Start** button, **Settings** and choose **Control Panel**.
2. Double click **Network connections** icon .
3. Select "**Local Area Connection"** from Network Connections. Right click on the icon and select "**Properties**".

4. Now, you have two setting methods:

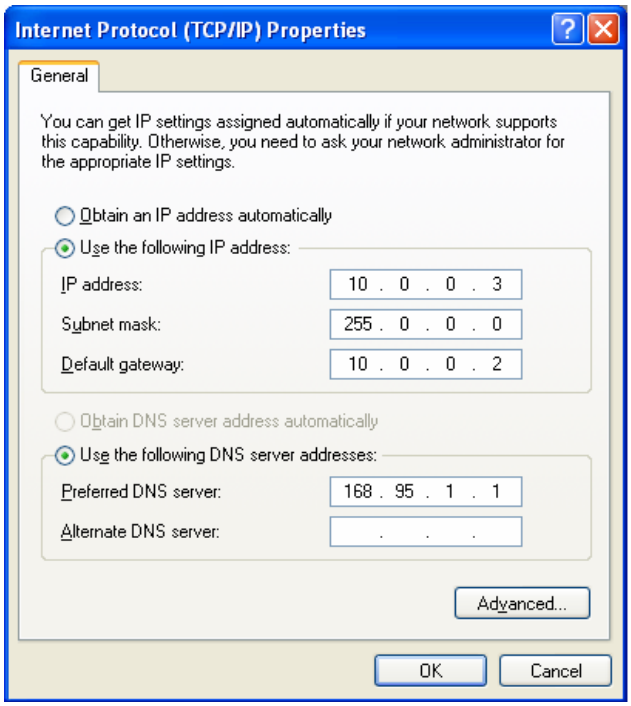
   A. Get IP Address from Router (DHCP)


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

   B. Configure IP Address manually.

   Select **Use the following IP address**. The default IP address of Router is 10.0.0.2. So please use 10.0.0.X (X is between 1 and 253, except 2) for IP address field and 255.0.0.0.0 for *Subnet Mask* field.

In the Default *Gateway* field, add the IP address of the Router (default IP is 10.0.0.2)


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 0 . 3
Subnet mask: 255 . 0 . 0 . 0
Default gateway: 10 . 0 . 0 . 2
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 168 . 95 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

Select **Use the following DNS server addresses.** Add DNS IP addresses which are provided by the ISP. Then click **OK** button.

Check your TCP/IP protocol

After configuring the TCP/IP protocol, you can use the ***ping*** command to check if your computer has successfully connected to this Router. The following example shows the ping procedure for Windows 98.

First, execute the ***ping*** command in MS-DOS Command prompt.

Ping 10.0.0.2

If the following messages appear:

- **Pinging 10.0.0.2 with 32 bytes of data:**
- **Reply from 10.0.0.2 : bytes=32 times<10ms TTL=64**
- **Reply from 10.0.0.2 : bytes=32 times<10ms TTL=64**
- **Reply from 10.0.0.2 : bytes=32 times<10ms TTL=64**

A communication link between your computer and this Router has been successfully established. Otherwise, if you get the following messages,

- **Pinging 10.0.0.2 with 32 bytes of data:**
- **Request timed out.**
- **Request timed out.**
- **Request timed out.**

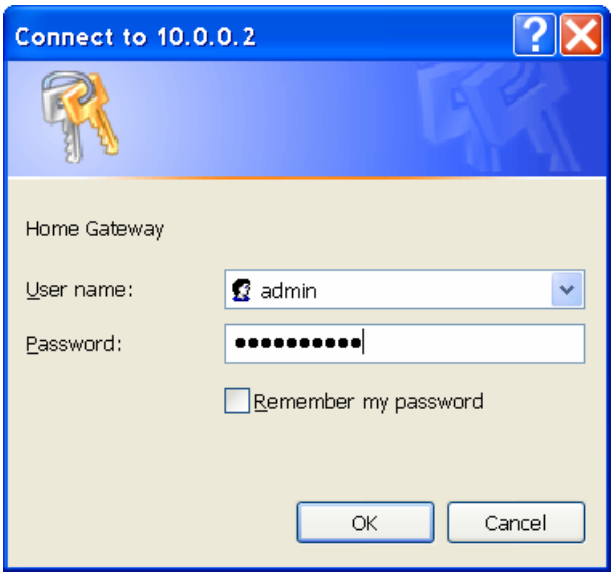
There must be something wrong in configuring procedure or cable issue. Please check the LAN LINK LED must be lighted. Or check TCP/IP configuration of your computer.

CHAPTER 5 ACCESS AND STATUS OF MODEM

The modem offers a web-based (HTML) graphical user interface allowing users to manage the Router using standard browser software such as Netscape Navigator or Microsoft Internet Explorer.

Accessing the Web Manager

- Launch the Web browser.
- Enter the LAN port default IP address http://10.0.0.2.
- Entry of the user name and password will be prompted. Enter the default **login User Name** and **Password**.
- The default login **User Name** of the administrator is **admin**, and the default login password is **epicrouter**.
- The default login **User Name** for the non-administrator is **user**, and the default login password is **password.**

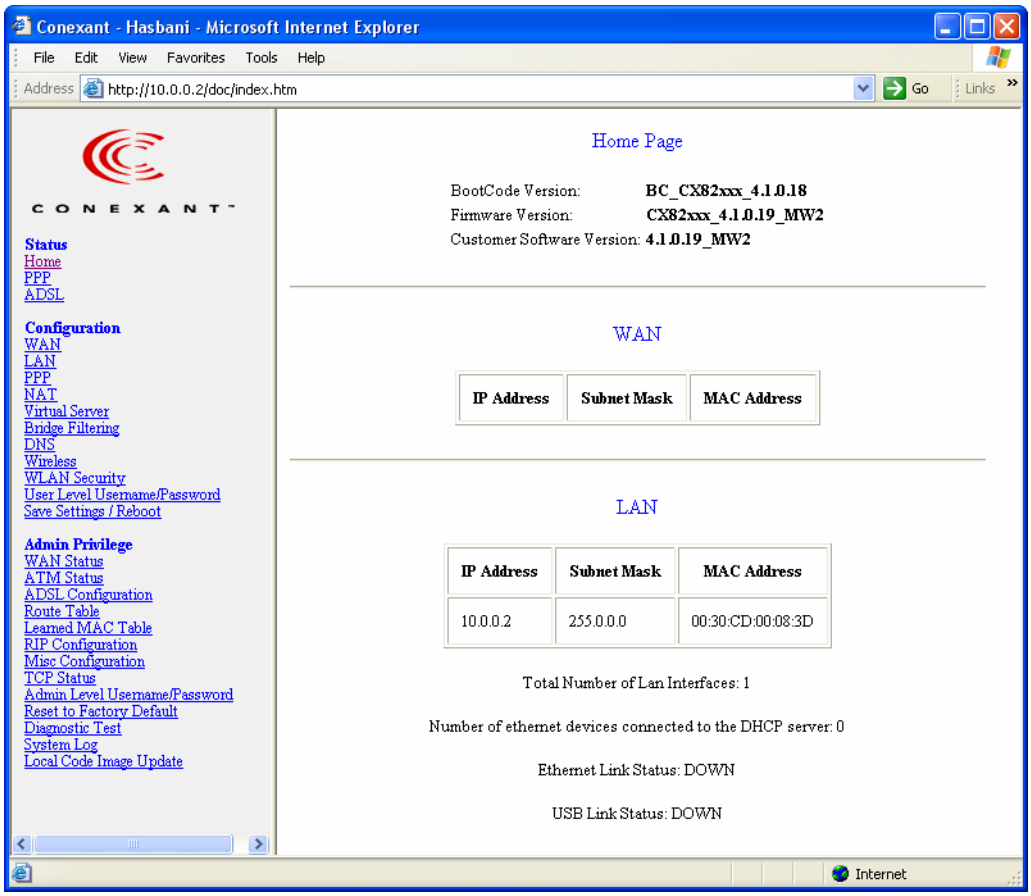


Modem Status

The links under the **Status** column are associated to the pages that represent the status of system and interfaces

Home Page

The **Home** page shows the firmware versions, WAN and LAN interface status. The **LAN** session shows the information and status of LAN port, DHCP client table, Ethernet link and USB link.

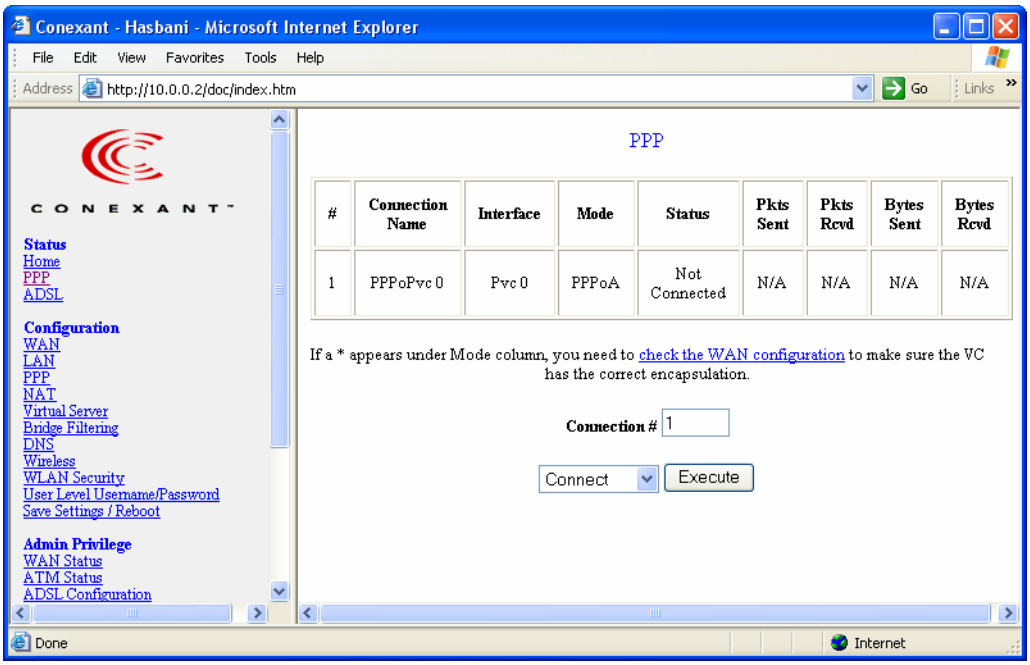


PPP Page

The **PPP Status** page shows the status of PPP for each PPP interface

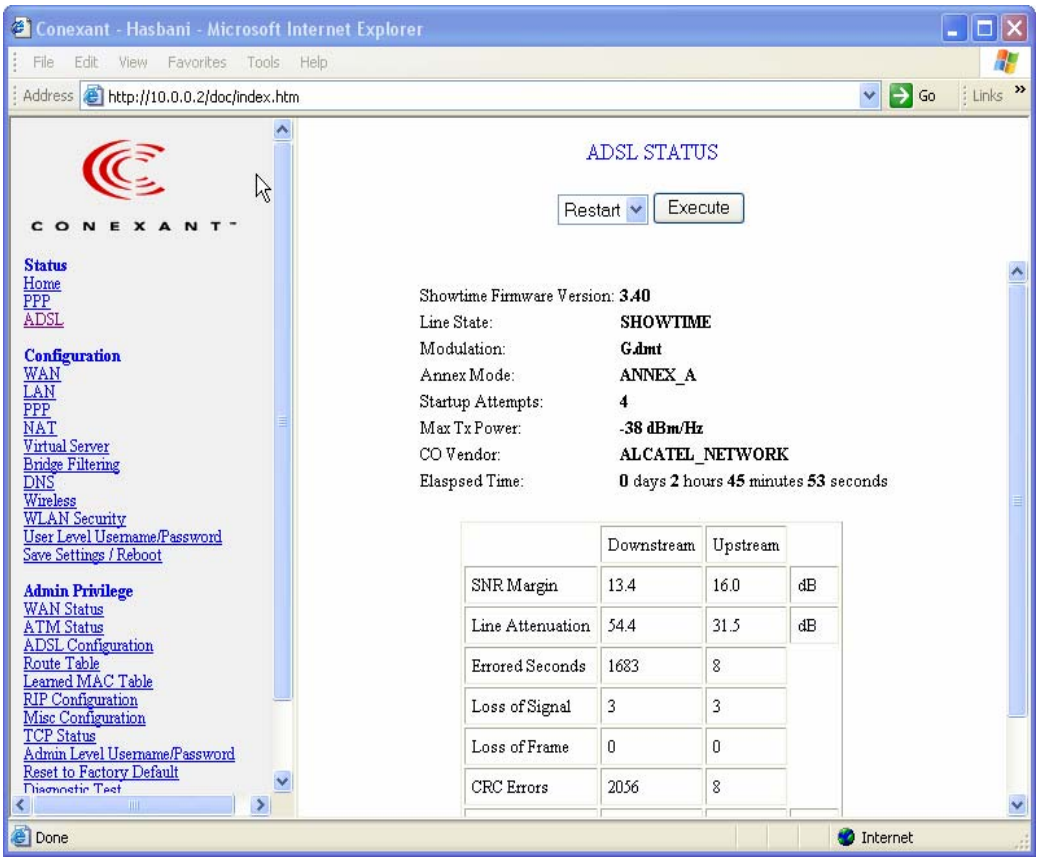
PPP: These fields display the Connection Name (user defined), Interface (PVC), Mode (PPPoE or PPPoA), Status (Connected or Not Connected), Packets Sent, Packets Received, Bytes Sent and Byte Received.

Connect and Disconnect: This field allows the user to manually connect/disconnect the PPP connection for each PPP interface. In another word, each PPP session can be connected and disconnected individually.



ADSL Status Page

The **ADSL Status** page shows the ADSL physical layer status.



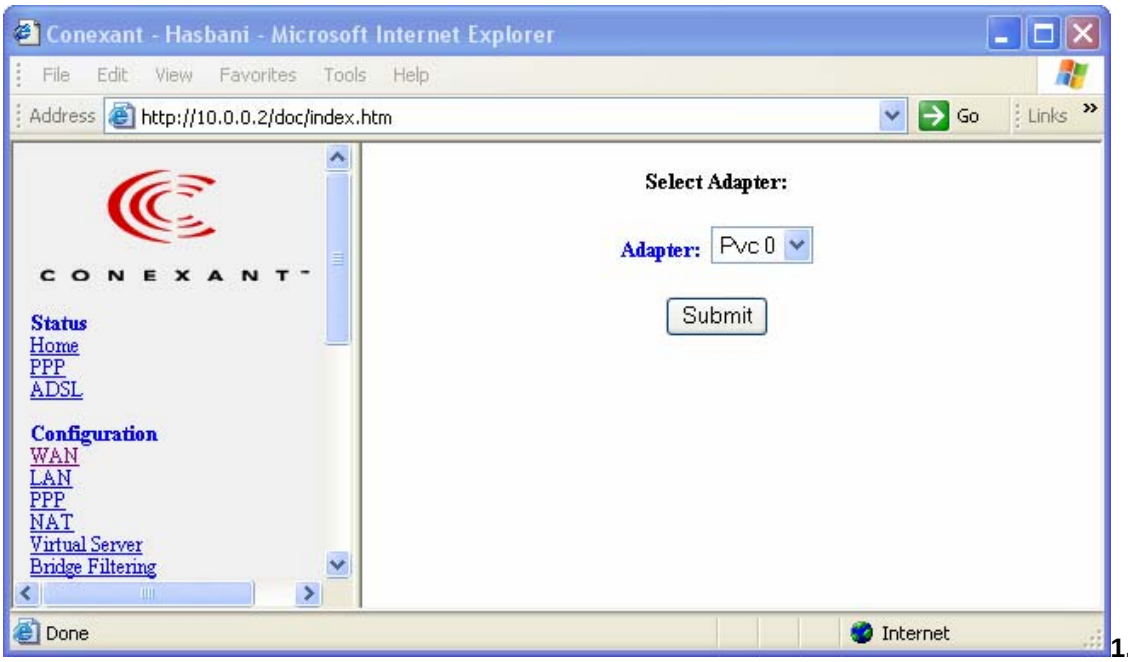
CHAPTER 6 CONFIGURE ADSL MODEM

The links under **Configuration** column are associated to the pages that represent the configurations of system and interfaces.

*Note: When the configurations are changed, please go to the **Save Settings** page to save the new setting and reboot modem.*

WAN Configuration

The **WAN** configuration page allows user to set the configuration for the WAN/ADSL ports. First, you select adapter, say, Pvc 0:

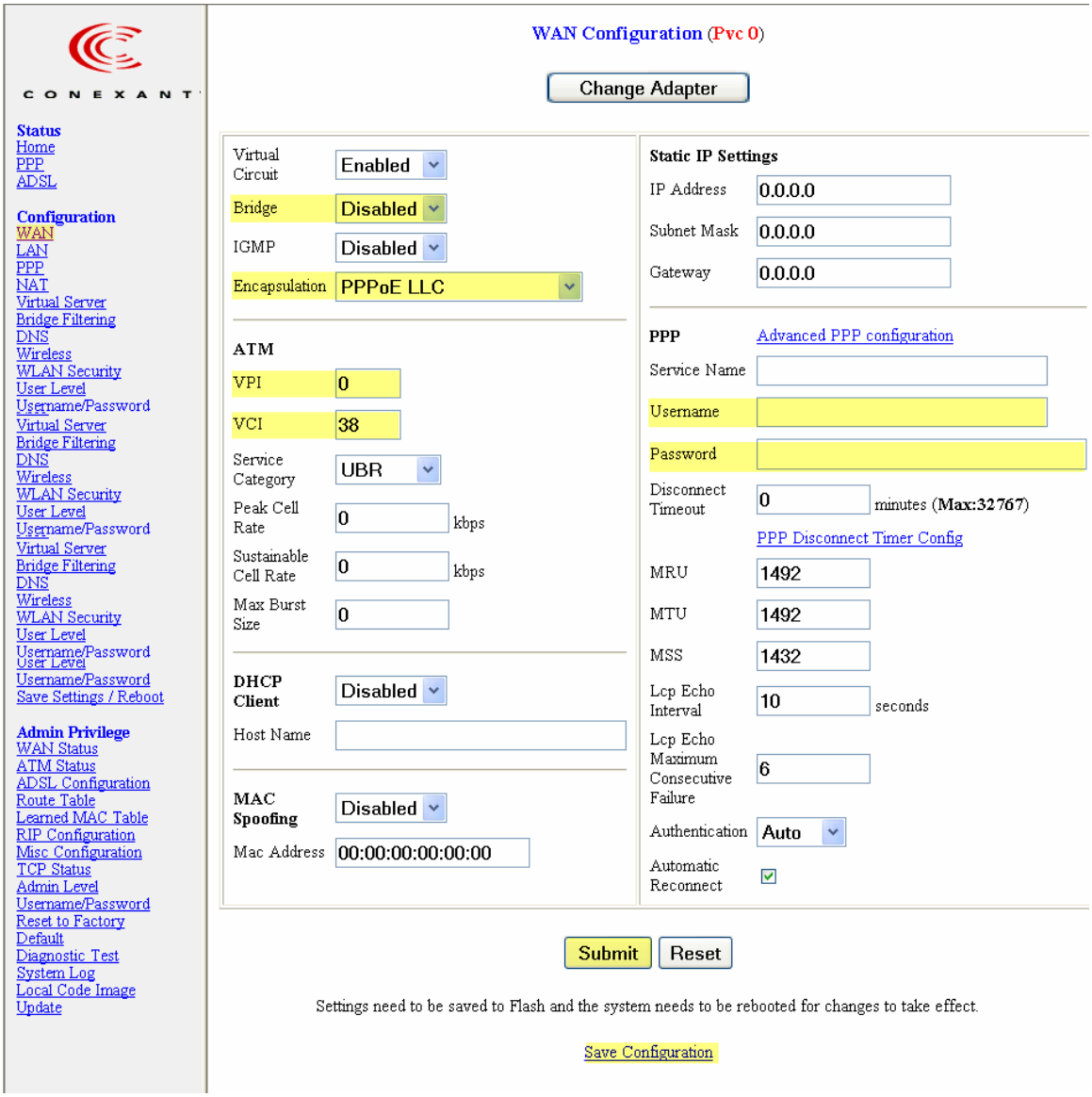


1. With Adapter (**Per Virtual Circuit) Setting**, it provides the configurations for IP address, Subnet Mask, Gateway and VPI/VCI. Current firmware supports eight PVCs. To switch between the PVCs, please choose the options of virtual circuit and click on the **Submit** button to switch over.

Once click Submit, WAN Configuration for Pvc 0 appears. Followings illustrate some popular setup for your modem.

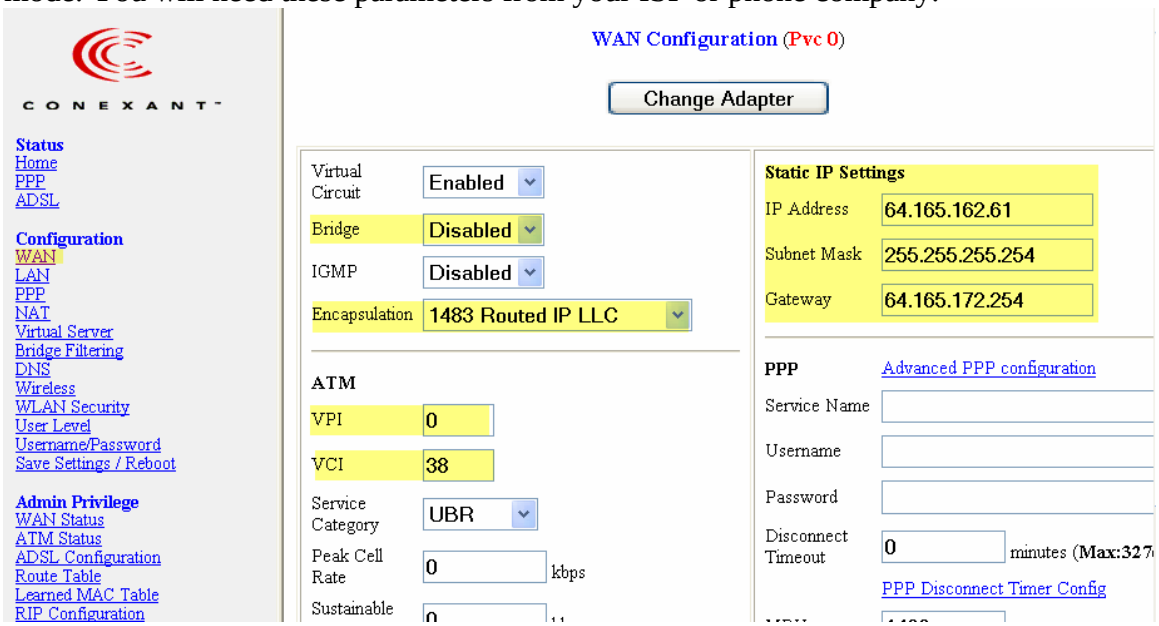
PPPoE / PPPoA mode with DHCP function

As shown on highlighted parameters, Enter VPI, VCI, User name, Password and Encapsulation. Disable Bridge mode and left other parameters unchanged. Click Submit, Save, then Reboot system. You will need these parameters from your ISP or phone company.



Router mode for Static IP with DHCP function

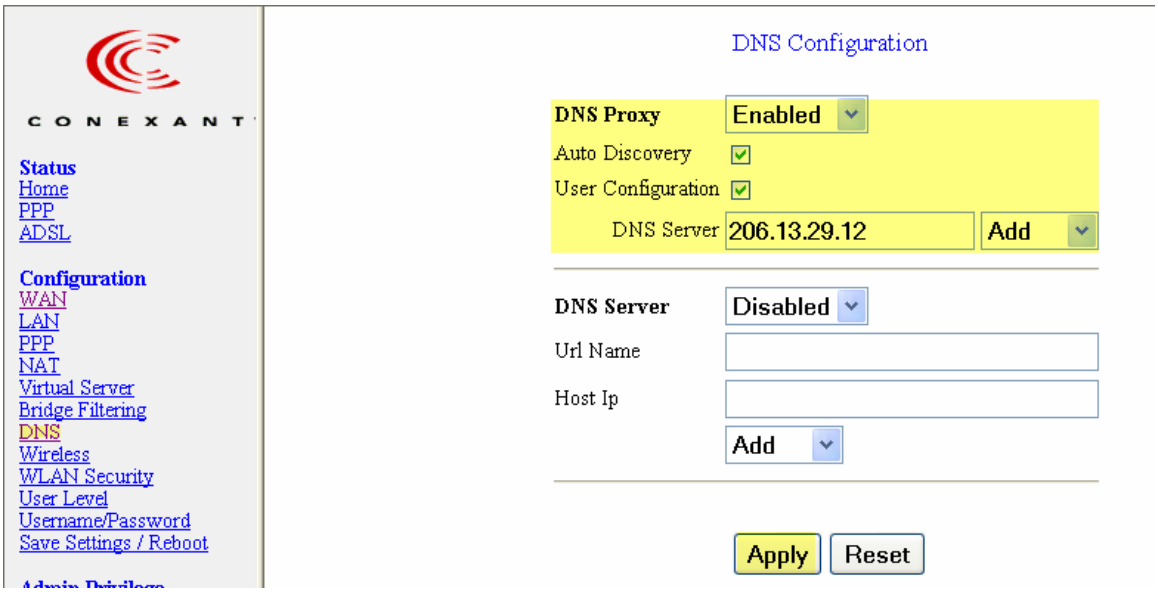
Enter Gateway, VPI, VCI, Static IP address, Subnet Mask, Encapsulation, disable Bridge mode. You will need these parameters from your ISP or phone company.



Note: The default IP address of this Router is 10.0.0.2. If you forget the modified IP address, you can't access this device anymore and the only solution is to reset it by pushing reset button.

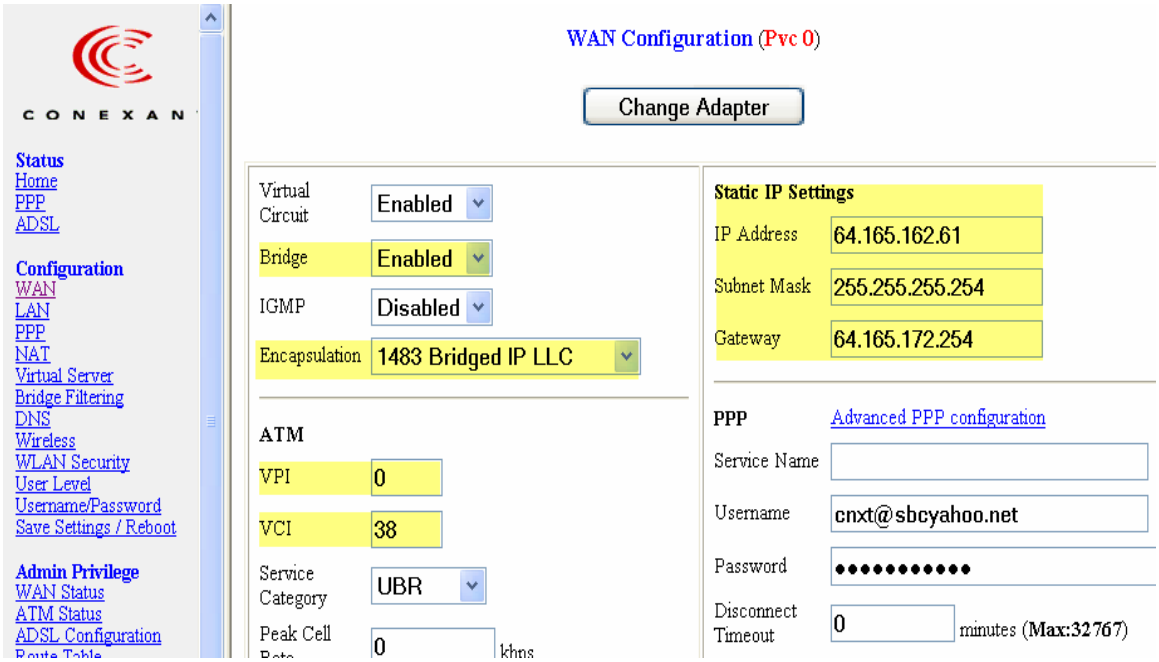
You may also need to enter DNS information if you can't access to internet:

- Click DNS page.
- DNS Proxy - Select Enabled,
- Select Auto Discovery
- User Configured and enter the DNS Server.
- Select Add, then Click Apply, Reboot.



Bridge mode with DHCP function

Enter VPI, VCI, Enable Bridge Mode, enter Encapsulation, IP, Subnet Mask, Gateway, and leave others unchanged. Save, Submit, then Reboot.



Additional Configuration of Router Modes

In a typical routed configuration, the ADSL router is treated as a separate device on the network that the PC and DSLAM send packets to. The Ethernet and ADSL networks are configured as separate IP subnets. The PC must have the ADSL router set up as its default gateway. Descriptions of the protocols supported in this mode of operation are discussed in the next sections.

Dynamic IP for WAN IP

Following settings are necessary when working under this mode:

- VPI/VCI
- Encapsulation: 1483 Bridged IP LLC
- Bridged: Disabled
- NAT Configuration: NAPT

Please see scenario 2: Router Mode Configuration with Dynamic IP in Appendix for more detail configuration.

Static IP for WAN IP

Following settings are necessary when working under this mode:

- VPI/VCI
- Static IP Address: provided by ISP
- Subnet Mask: provided by ISP
- Default Gateway: provided by ISP
- Encapsulation: 1483 Bridged IP LLC or 1483 Routed IP LLC (provided by ISP)
- Bridged: Disabled
- NAT Configuration: NAPT
- Preferred DNS server: IP is Provided by ISP

Please see scenario 3: Router Mode Configuration with Static IP in Appendix for more detail configuration.

PPPoA (RFC 2364)

PPP is a widely used protocol for controlling a point-to-point link. It is used by existing ISPs (Internet Service Providers) in providing dial-in services for the Internet. It can be used over a variety of physical media to transport IP data, MAC data, and many other data types. Components of PPP have been defined which provide option negotiation, compression, encryption, authentication and multi-link facilities. For Xdsl deployment, authentication is probably the single most important of these.

Following settings are necessary when working under this mode:

- VPI/VCI
- Encapsulation: PPPoA VC-Mux
- Bridged: Disabled
- PPP User Name: Provided by ISP

- PPP password: Provided by ISP
- NAT Configuration: NAPT

Please see scenario 4: Router Mode Configuration PPPoA in Appendix for more detail configuration.

PPPoE (RFC 2516)

Following settings are necessary when working under this mode:

- VPI/VCI
- Encapsulation: PPPoE LLC
- Bridged: Disabled
- PPP User Name: Provided by ISP
- PPP password: Provided by ISP
- NAT Configuration: NAPT

Please see scenrio 5: Router Mode Configuration PPPoE in Appendix for more detail configuration.

Classical IP over ATM (RFC 1577)

Following settings are necessary when working under this mode:

- VPI/VCI
- Static IP Address: provided by ISP
- Subnet Mask: provided by ISP
- Default Gateway: provided by ISP
- Encapsulation: Classical IP over ATM
- Bridged: Disabled
- NAT Configuration: NAPT
- Preferred DNS server: IP is Provided by ISP

Please use following table to configure a valid setting for each of PVC, or go to Appendix page to choose the suitable scenario.

WAN Configuration	Bridge Mode	Router Mode (PPPoA/PPPoE)	Router Mode (Dynamic IP)	Router Mode (Static IP)
IP address	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
Subnet Mask	N/A	Automatically assigned by ISP	Automatically assigned by ISP	Provided by ISP
Encapsulation	1483 Bridged IP LLC,1483 Bridged IP VC-Mux	PPPoA LLC/VC-Mux, PPPoE LLC/VC-Mux	1483 Bridged/Routed IP LLC,1483 Bridged/Routed IP VC-Mux, Classical IP over ATM	1483 Bridged/Routed IP LLC,1483 Bridged/Routed IP VC-Mux, Classical IP over ATM
Bridge	Enabled	Disabled	Disabled	Disabled
PPP Service	N/A	Provided by ISP	N/A	N/A
PPP User Name	N/A	Provided by ISP	N/A	N/A
PPP Password	N/A	Provided by ISP	N/A	N/A
DHCP Client enable	Unchecked	Unchecked	Checked	Unchecked

Per VC Settings

Under **Per VC Setting**, it provides the configurations for IP address, Subnet Mask, Gateway and VPI/VCI. Current firmware supports eight PVCs. To switch between the PVCs, please choose the options of virtual circuit and click on the **Submit** button to switch over.

Bridge Mode

In a typical bridged configuration, the ADSL router is transparent to the network. It bridges the ADSL line to the Ethernet line making both side appear as a single subnet. In this configuration, an IP address only needs to be provided to the PC. It may still be beneficial to provide an IP address to the ADSL router for management.

Following settings are necessary when working under this mode:

- VPI/VCI
- Encapsulation: 1483 Bridged IP LLC
- Bridged: Enabled
- NAT Configuration: Disabled
- LAN DHCP Server: Disabled

Please see scenario 1: Bridge Mode Configuration Table in Appendix for more detail configuration.

IGMP

IGMP relay/proxy specification and environment:

- Support IGMP proxy/relay function for ADSL modem, based on the following requirement and case.
- On CO side, there must be at least one IGMP querier (router) present. IGMP querier will send IGMP query packet. The ADSL modem is responsible to relay these IGMP query to Ethernet.
- End-user multicast application device send IGMP report while receiving IGMP query or being activated by user, the ADSL modem should be responsible to proxy (that is, change source IP to ADSL modem's WAN IP) the IGMP report to ADSL WAN side, include all PVCs. The same case is for IGMP leave packet.
- Not necessary to relay multicast routing between two ADSL PVCs or two interfaces in LAN side.
- Special purpose multicast packet (such as RIP 2 packet) should run without interference.

Table for Packet Process

Rx Entity	Packet Class	TTL	Action	Notes
ADSL	IGMP query	1	Relay to Ethernet	
	IGMP report	1	Ignore	
	IGMP leave	1	Ignore	
	General Multicast IP	-	Relay it to Ethernet.	
Ethernet	IGMP query	1	Ignore	
	IGMP report	1	Relay to all ADSL PVC	
	IGMP leave	1	Relay to all ADSL PVC	
	General Multicast IP	-	Ignore	

Note: Before the IGMP mode is enabled; please go to the **Miscellaneous Configuration** page to enable the IGMP proxy. Otherwise, the IGMP selection will not be valid.

ATM

- **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by aneight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
Range for VPI field is 0-255, default is 0.

- **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
Range for VCI field is 0-65535, default is 38.

- **Service Category:** This field allows you to select from the following service categories, with UBR as the default.
    - UBR (Unspecified Bit Rate): When configured as UBR, traffic is delivered with best efforts but with no guarantee. This allows for fluctuation in times of temporary increase of available bandwidth. For example, if a PVC with CBR is temporarily inactive, the PVC(s) with UBR will utilize that bandwidth while it is available. UBR is intended for applications that do not require any maximum bound on the transfer delay.
    - CBR (Constant Bit Rate): When a PVC is specified as a CBR, that PVC is guaranteed a certain bandwidth, characterized by the Peak Cell Rate (PCR). The CBR does not have to transmit with a peak cell rate, and when it does, it is only when the bandwidth specified by the PCR is guaranteed.
    - VBR-nrt (Variable Bit Rate - non real time): An PVC enabled with VBR-nrt can transmit a cell only if the PVC has a token available. The PVC accumulates tokens at the rate of the **Sustainable Cell Rate**, and the PVC can only accumulate a maximum of the value specified by **Maximum Burst Size** tokens. When a PVC has a token available, it can transmit cells at the rate of PCR. After a cell is transmitted, the PVC loses the token it has accumulated.
    Note: In the case of multiple PVCs, CBR specified PVCs will have higher priority than PVCs with UBR. For example, the CBR PVCs will take their bandwidth and the remaining bandwidth will be split among the UBR PVCs. In the case of total PVC CBR bandwidth exceeding ADSL upstream, the total upstream bandwidth will be shared proportionally to the bandwidth allocated for each CBR PVC.

- **Peak Cell Rate:** This value specifies the maximum, and in some cases guaranteed, cell rate for CBR and VBR-nrt. Peak Cell Rates are typically measured in Cells/Second, however, the user entered value is in kbps and is then converted by the firmware.
Range for Peak Cell Rate field is 0-32767, default is 0.

- **Sustainable Cell Rate:** This is the sustained rate at which a PVC enabled with VBR-nrt can transmit ATM cells. Sustainable Cell Rate (SCR) can be considered as the true reserved bandwidth for a PVC.
Range for Sustainable Cell Rate field is 0-32767, default is 0.
- **Max Burst Size:** This is the number of cells a PVC enabled with VBR-nrt can transmit continuously at peak cell rate (PCR).
Range for Max Burst Size field is 0-32767, default is 0.

Example: CBR and UBR
This example is provided to further explain the dynamics of UBR and CBR and how different PVCs with different service category specifications coexist. In this example, the ADSL upstream is 900 kbps.

Sample Configuration		
PVC	Service Category	Peak Cell Rate
0	CBR	400 kbps
1	CBR	800 kbps
2	UBR	N/A
3	UBR	N/A

Scenario	Actual (Adjusted) Bandwidth Usage
PVC0 is busy PVC1 is idle PVC2 and PVC3 are busy	PVC0 uses 400 kbps PVC2 uses 250 kbps PVC3 uses 250 kbps
PVC0 is idle PVC1 is busy PVC2 and PVC3 are busy	PVC1 uses 800 kbps PVC2 uses 50 kbps PVC3 uses 50 kbps
PVC0 is busy PVC1 is busy PVC2 and PVC3 are busy	PVC0 uses 300 kbps PVC1 uses 600 kbps PVC2 uses 0 kbps PVC3 uses 0 kbps

Example: VBR-nrt
This example is provided to further explain the dynamics of VBR-nrt A PVC has a service category of VBR-nrt with the following parameters:
1. PCR = 400 kbps
2. SCR = 100 kbps
3. MBS = 22 cells (Note that 22 cells * 48 bytes/cell = 1056 bytes)

If the PVC has been idle for a while (meaning it has accumulated a MBS of 22 cells), and it just has two packets of the same size (1000 bytes) to send. It can transmit the first packet of size (1000 bytes) in 20ms: (1000 bytes * 8bit/byte / 4000kbps). Immediately after the first second packet is transmit, it will take about 80ms to transmit the second packet because the PVC can only transmit the second packet at SCR (100kbps).

DHCP Client

DHCP Client: This is to enable or disable (default) the ADSL Bridge/Router WAN as a DHCP client, where the ISP would be the DHCP server. DHCP Client is generally used in the following encapsulations: 1483 Bridged IP LLC, 1483 Routed IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP VC-Mux, and Classical IP over ATM. This option is for non-static (dynamic) IP addresses.

Host Name: When DHCP Client is Enabled, copy the ISP recognized Host Name here. The Host Name can be up to 19 characters.

Enable this if your modem is a client of DHCP server provided by your ISP.

Host name: Required by some ISPs. If the ISP does not provide the Host name, please leave it blank.

MAC Spoofing

MAC Spoofing: Enable MAC Spoofing to make a different MAC Address appear on the WAN side. This is also used to solve the scenario where the ISP only recognizes one MAC Address.
Default is Disabled.

MAC Address: When MAC Spoofing is enabled, copy the ISP-recognized MAC address here. Format for MAC address is six pairs of hexadecimal numbers (0-9, A-F) separated by colons.
Default is 00:00:00:00:00:00.

Static IP Settings

Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

IP Address: This is the static IP Address given by the ISP.
Range for IP Address is x.x.x.y, where 0 ≤ x≤ 255 and 1 ≤ y≤ 254, default is 0.0.0.0

Subnet Mask: This is the subnet mask given by the ISP.
Range for Subnet Mask is x.x.x.x, where 0 ≤ x≤ 255, default is 0.0.0.0

Gateway: This is the Gateway given by the ISP.
Range for Gateway is x.x.x.y, where 0 ≤ x≤ 255 and 1 ≤ y≤ 254, default is 0.0.0.0.

PPP Configuration

The current release supports multiple PPP sessions per PVC. The PPP configuration in the WAN configuration page is for the first PPP session for each of PVC. The predefined PPP Account Name (Account ID) is “Simple PPP Account 0” for PVC0 and predefined PPP Connection Name is “Simple PPP Session 0” for PVC0. For the other PVC X, the predefined account name and connection name will be Simple PPP Account X and Simple PPP Session X. X is the PVC number from 1 to 7.
It can support up to total of 16 PPP sessions, and each of PVC can support up to 8 PPP sessions. The multiple PPP sessions may be configured with any combination over 8 PVCs.

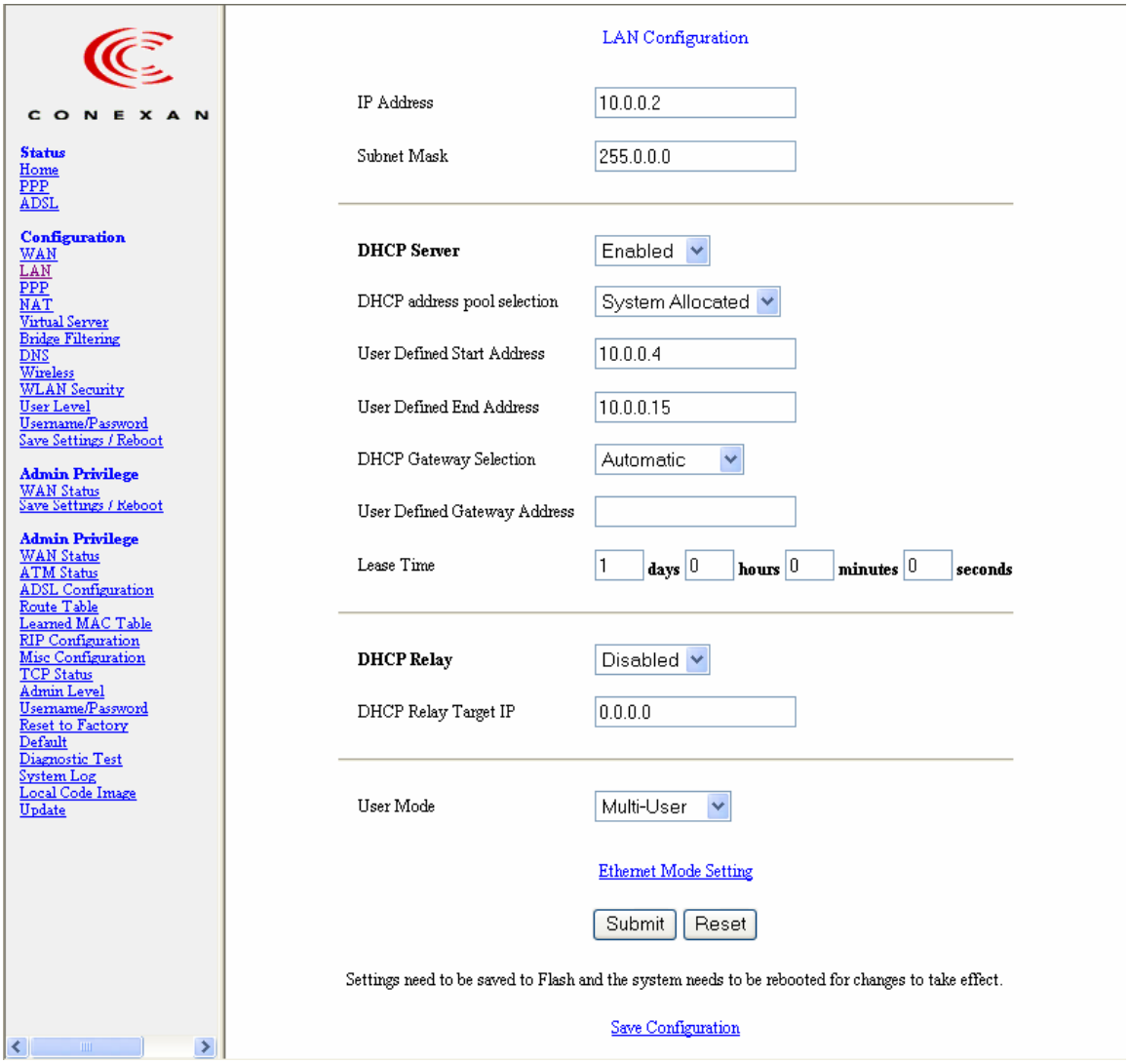
- Service Name: The service name of PPP is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.
- User Name: Enter the PPP user name (usually provided by the ISP).
  Note: You cannot have two different user accounts with the same account name. If a different User Name with an already existing Account ID is submitted, it will replace the previous account with that Account ID. You can have the same User Name and Password for two different accounts (Account ID).
- Password: Enter the PPP password (usually provided by the ISP).
- Disconnect Timeout: The Disconnect Timeout allows users to set the specific period of time to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

Please refer to following session for more detailed information about PPP configuration.

LAN Configuration

The **LAN** configuration page allows user to set the configuration for the LAN port.

The modem comes with a preset default IP address setting of 10.0.0.2 for the LAN port. There are two ways to use this default IP address, you can manually assigned an IP address and subnet mask for each PC on the LAN or you can instruct the Router to automatically assign them using DHCP. The DHCP function is active by default.



- LAN IP Address & Subnet Mask: The default is 10.0.0.2 and 255.0.0.0. User can change it to other private IP address, such as 192.168.1.2, and 255.255.255.0.

- **DHCP Server**

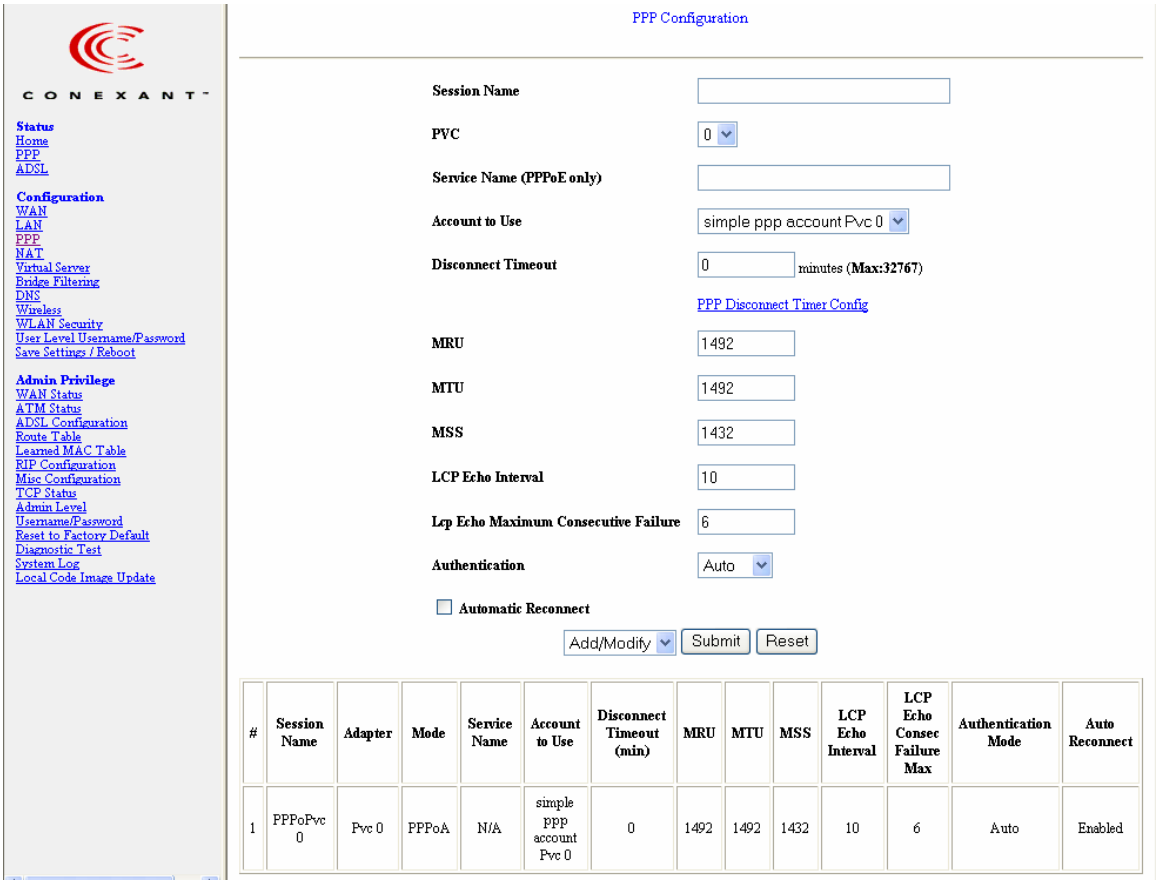
- **System Allocated:** The DHCP address pool is based on LAN port IP address plus 12 IP addresses. For example, the LAN IP address is 10.0.0.2; the DHCP address pool is at the range of 10.0.0.3 to 10.0.0.14.
- **User Defined:** The DHCP address pool is at the range of User Defined Start Address and User Defined End Address. The maximum pool size can be 253 IP addresses: 255 total IP addresses – 1 broadcast address – 1 LAN port IP address.
- **Lease time:** The Lease time is the amount of time of a network user will be allowed to connect with DHCP server. If all fields are 0, the allocated IP addresses will be effective forever.

- **DHCP Relay:** If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please disable the NAT to run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

- **User mode:** Under the **Single User** mode, the DHCP server only allocates one IP address to local PC. Under the **Multiple User** mode, the DHCP server allocates the IP addresses specified bye the DHCP address pool.

PPP Configuration

The PPP Configuration page allows you to configure multiple PPP sessions for each of PVC. It can support up to total of 16 PPP sessions, and each of PVC can support up to 8 PPP sessions. The multiple PPP sessions may be configured with any combination over 8 PVCs. To configure the PPP, must go to the PPP Account Configuration page first to configure Account ID, Users Name and Password.



- **Session Name:** This field allows you to enter a Session Name. This is user defined to help distinguish different session for different PPP accounts and different PVCs.
- **PVC:** This field allows you to choose the specific PVC for the PPP session.
- **Service Name:** The Service Name of the PPP session is required by some ISPs. If the ISP does not provide the Service Name, please leave it blank.
- **Account to Use:** You must select an account created in **PPP Account Configuration** page here.
- **Disconnect Timeout:** The Disconnect Timeout allows you to set the specific period of time, in minutes, to disconnect from the ISP. The default is 0, which means never disconnect from the ISP.

Range for Disconnect Timeout field is 0-32767, default value is 0.

- **PPP Disconnect Timer Configuration** page, see following section.

- **MRU:** The MRU (Maximum Receive Unit) field indicates the maximum size IP packet that the peer of PPP connection (this device) can receive. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.
Range for MRU field is 0-32767, default value is 1492.
- **MTU:** Maximum Transmission Unit (MTU) is the largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).
Range for MTU field is 0-32767, default value is 1492.
- **MSS:** Maximum Segment Size is the largest size of data that TCP will send in a single, unfragmented IP packet. The LAN client and the WAN host will indicate their MSS during the TCP connection handshake.
Range for MSS field is 0-32767, default value is 1432.
- **Lcp Echo Interval:** This is the time interval, in seconds, between PPP session connection attempts.
Range for Lcp Echo Interval field is 0-32767, default value is 10.
- **Lcp Echo Maximum Consecutive Failure:** This is the number of times a PPP session can fail while trying to connect before stopping. If a PPP session fails this number of times, you must manually reconnect the PPP session.
Range for Lcp Echo Maximum Consecutive Failure field is 0-32767, default value is 6.
- **Authentication:** The different types of available authentications are:
    - Auto: When auto is selected, PAP mode will run by default. However, if PAP fails, then CHAP will run as the secondary protocol. This is the default setting.
    - PAP: Password Authentication Procedure. Authentication is done through username and password.
    - CHAP: Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.
- **Automatic Reconnect:** When it is checked, the ADSL Bridge/Router will reconnect a PPP session when it is terminated by the ISP. If a PPP session is terminated under any other conditions (i.e. by Disconnect Timeout or manual disconnect), the Automatic Reconnect will not reconnect the session. This box is unchecked by default.
- **PPP Configuration Status:** A table will be displayed at the bottom of this page to show all the Session Names with its Adapter (PVC number), Mode (PPPoA or PPPoE), Service Name, Account to Use (PPP Account ID), Disconnect Timeout configuration, MRU, MTU, MSS, Authentication Mode (Auto, CHAP or PAP), and Auto Reconnect configuration.

PPP Disconnect Timer Configuration

The PPP Disconnect Timer Configuration page enables you to configure what action will bring a PPP Session out of the Idle state (disconnected state) and reset the Idle Timer. This is done by specifying criteria contained in packets, namely IP Protocol and Port. The Idle Timer refers to the Disconnect Timeout, specified on the PPP Configuration page. The PPP Idle Timer is recommended to be disabled (**Disconnect Timeout** = 0 on PPP Configuration page) if you want an always on connection. **PPP Disconnect Timer Configuration** is intended for users who do not desire an always on connection and/or their ISP charge by connection time.

Enable/Disable Idle Timer Filter

All Traffic will reset Idle Timer (ignore filter below): Selecting this option will disable the PPP Idle Timeout filter and allow any traffic through any protocol or port to reset the idle timer. The only dependency is that the traffic must correspond with the Filter Application (Inbound and/or Outbound). For example, if **Outbound Traffic Only** is selected, only traffic in the outbound direction will reset the idle timer. When this option is selected, all user configured criteria (displayed in the filter table) is bypassed.

Only filtered traffic will reset the Idle Timer (use filter below): Selecting this option will enable the PPP Idle Timeout filter and only allow traffic specified in the filter table to reset the idle timer. The traffic specified in the filter table must also correspond with the Filter Application selection. For example, outbound traffic with criteria matching that of the filter table will only be allowed to pass if either **Outbound Traffic Only** or **Inbound and Outbound Traffic** is selected.
Note: PPP reconnect on WAN access must be enabled for the Idle Timer to reconnect a PPP Session when a request is made from the LAN to the WAN.

Filter Application

The Filter Application consists of three options that determine which sources (LAN and/or WAN) will be able to reset the Idle Timer and reconnect the PPP session.

- **Inbound Traffic Only:** Selecting this option will allow PPP requests from the WAN side to reset the **Disconnect Timeout** timer. Note that requests from the WAN side cannot bring a PPP Session out of Idle state. This is because when a PPP Session is in Idle state, the connection is down (if they match the filter table criteria).
- **Outbound Traffic Only:** When this option is selected (default), PPP sessions can only be activated (Idle Timeout) when a request is made on the LAN side to the

WAN side. The disconnect timer will reset when outbound traffic is detected (if they match the filter table criteria).

- **Inbound and Outbound Traffic:** Selecting this will allow both WAN and LAN source packets to reset the idle timer.

Filter Details

The table displayed in the Filter Details section of the page shows all the current Idle Filters. Traffic must match the criteria of one of these filters in order to cause an Idle Timeout, unless **All Traffic will reset Idle Timer** is selected. As a default and starting point for configuration, WWW browsing (HTTP), FTP, and Telnet related packets are part of the filter table.

- **IP Protocol:** This is the IP Protocol name corresponding to the Protocol Number.
- **Protocol #:** This is the IP protocol (number) through which the PPP session can be activated. The Protocol Numbers for filters are:
    - TCP Protocol Number: 6
    - UDP Protocol Number: 17
    - ICMP Protocol Number: 1
    - IGMP Protocol Number: 2
- **Port #:** This is the Port through which the PPP session can be activated. The default filters are:
    - HTTP TCP Port: 80
    - FTP TCP Port: 20 and 21
    - Telnet TCP Port: 23
    - DNS UDP: 53
- **Action:** You can add a rule by entering the appropriate information, selecting **Add** on the **Action** dropdown menu, and clicking **Submit**. To delete an entry, you can enter the information of an entry that already exists on the table, select **Delete** on the **Action** dropdown menu, and click **Submit**.

PPP Disconnect Timer Configuration

The settings on this page are used to determine the traffic that will:

1) Reset the PPP disconnect timer counter
2) Re-establish a PPP connection (only if "PPP Reconnect on WAN Access" is enabled)

Enable/Disable Idle Timer Filter

- ○ All Traffic will reset Idle Timer (ignore filter below)
- ◉ Only filtered traffic will reset Idle Timer (use filter below)

execute

Apply Filter To:

- ○ Inbound Traffic Only
- ◉ Outbound Traffic Only
- ○ Inbound and Outbound Traffic

execute

Filter Details:

Protocol #	Port #	Action
0	0	Add

Submit Reset

#	IP Protocol	Protocol #	Port #
1	TCP	6	80
2	TCP	6	23
3	TCP	6	21
4	TCP	6	20
5	UDP	17	53

Number of Entries is 5

Clear All Restore to Default

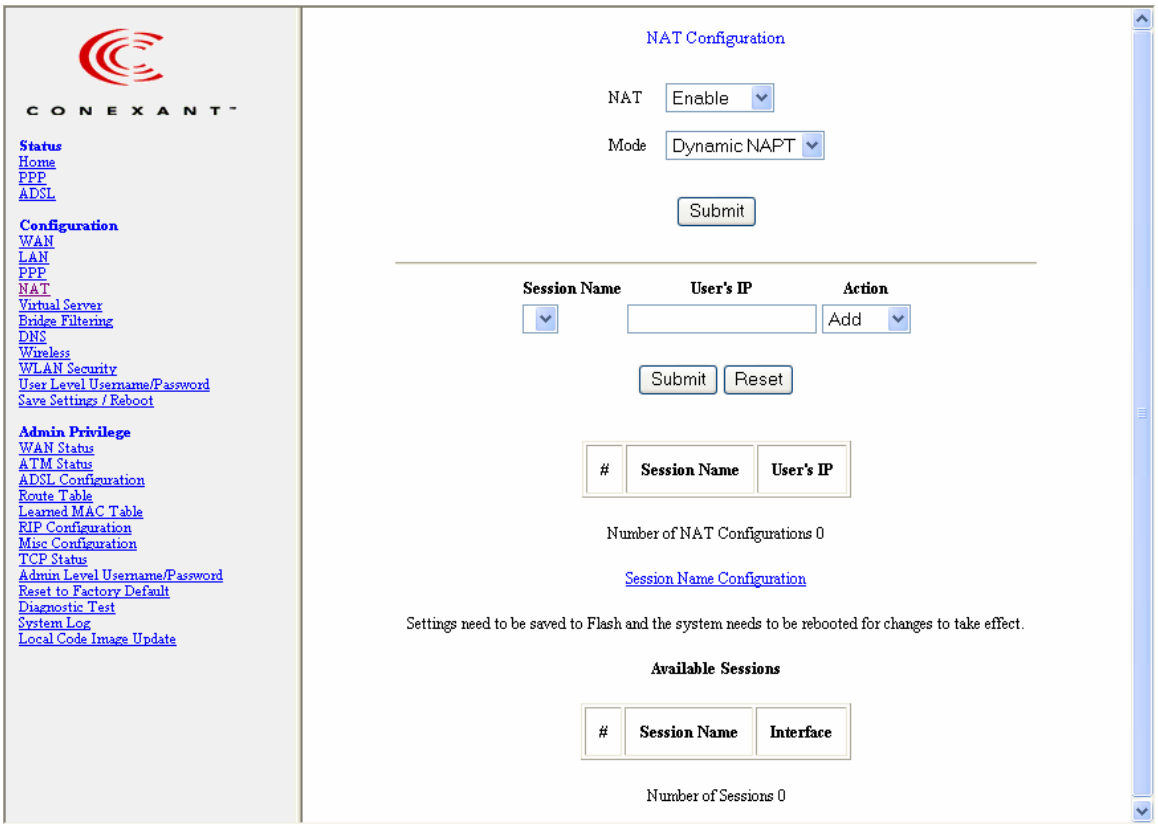
Well Known Ports

Application	Port Number
Any	0
FTP-Data	TCP 20
FTP-Control	TCP 21
Telnet	TCP 23
SMTP	TCP 25
HTTP	TCP 80
DNS	UDP 53

NAT Configuration

The NAT Configuration page allows the user to set the configuration for the Network Address Translation. The default setting is Dynamic NAPT. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.

When the Dynamic NAPT is chosen, there is no need to configure the NAT Session and NAT Session Name Configuration.



NAT (Static)

The NAT option only maps single WAN IP address to the local PC IP address. It is peer-to-peer mapping. (1x1) For each WAN interface, only one local PC IP address can be associated with each WAN interface. Click the link Session Name Configuration to add the session name for WAN interface.

- **Session Name**: This field allows the user to enter his/her own session Name to distinguish different NAT session for different interfaces among different PPP sessions and different PVCs.

- **Interface**: This field allows the user to choose specific WAN Interface (PVC or PPP Session) for NAT Session.
- **NAT Session Name Status** will be displayed at the bottom of this page to show all the Session Names with its WAN Interface.
- Click the link **Go back to NAT Configuration** to the NAT configuration page. Select the **NAT** option. Input the session name and the PC IP address, and choose the **Add** action. Click the **Submit** button and go to the **Save Settings** to save this configuration.
  NAT allows only one entry (User IP) per session.
- **Session Name Status** will be displayed at the middle of this page to show the corresponding Session Name with its IP address.
- **Available Sessions Status** will be displayed at the end of this page to show all the Session Names with its WAN Interface.

NAPT (Static)

The NAPT option maps the single WAN IP addresses to many local PCs IP addresses. (1Xn). It is the multiple-mapping mechanism. For each WAN Interface, more than one local PCs can be associated with one WAN Interface. Click the link Session Name Configuration to add the session name for WAN interface.

- **Session Name:** This field allows the user to enter his/her own session Name to distinguish different NAT session for different interfaces among different PPP sessions and different PVCs.
- **Interface**: This field allows the user to choose specific WAN Interface (PVC or PPP Session) for NAT Session.
- **NAT Session Name Status** will be displayed at the bottom of this page to show all the Session Names with its WAN Interface.
- Click the link **Go back to NAT Configuration** to the NAT configuration page. Select the **NAPT** option. Select the Session Name and assign the PC IP address, and choose the Add action. Click the Submit button and go to the Save Settings to save this configuration.
- **NAPT allows many entries (User IPs) per session.**
- **Session Name Status** will be displayed at the middle of this page to show the corresponding Session Name with its IP address.
- **Available Sessions Status** will be displayed at the end of this page to show all the Session Names with its WAN Interface.

Virtual Server

The **Virtual Server Configuration** page allows users to set the configuration of Virtual Server. The firmware includes the Free BSD version firewall. All UDP/TCP ports are protected from intrusion. If any specific local PCs need to be mapped to the UDP/TCP port on WAN side, please input the mappings here.

This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the virtual server.

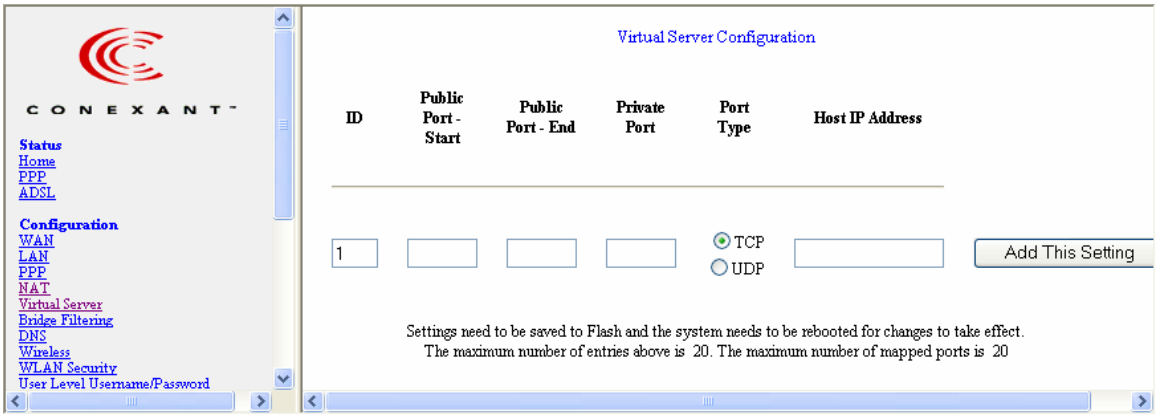
The Virtual Server allows you to set up public services, such as a Web server, FTP, E-mail etc. that can be accessed by external users of the Internet. Each service is provided by a dedicated network computer configured with a fixed IP address.

Set up private network computers to act as servers and configure each server with a fixed IP address. Enter the desired service port numbers in the public port and private port field and specify port type as TCP or UDP.

Well-known ports are

Port number	Service	Port number	Service
7	Echo	79	Finger
20,21	FTP	80	HTTP
23	Telnet	110	POP3
25	SMTP	161	SNMP
53	DNS	162	SNMP Traps

Click" Add this setting" button after you set and click "save settings" to save all configuration.



- **Public Port**: This field allows the user to enter the port number of the Public Network.
- **Private Port**: This field allows the user to enter the port number of the Private Network. In most cases, the private port number is same as public port number.
- **Host IP Address**: This field allows the user to enter the private network IP address for the particular sever.

For example, IP of Windows machine that connected with modem is 192.168.2.101 and you want to disable port 21 with UDP protocol:

ID	Public Port	Private Port	Port Type	Host IP Address
2	21	21	choose UDP	192.168.2.101

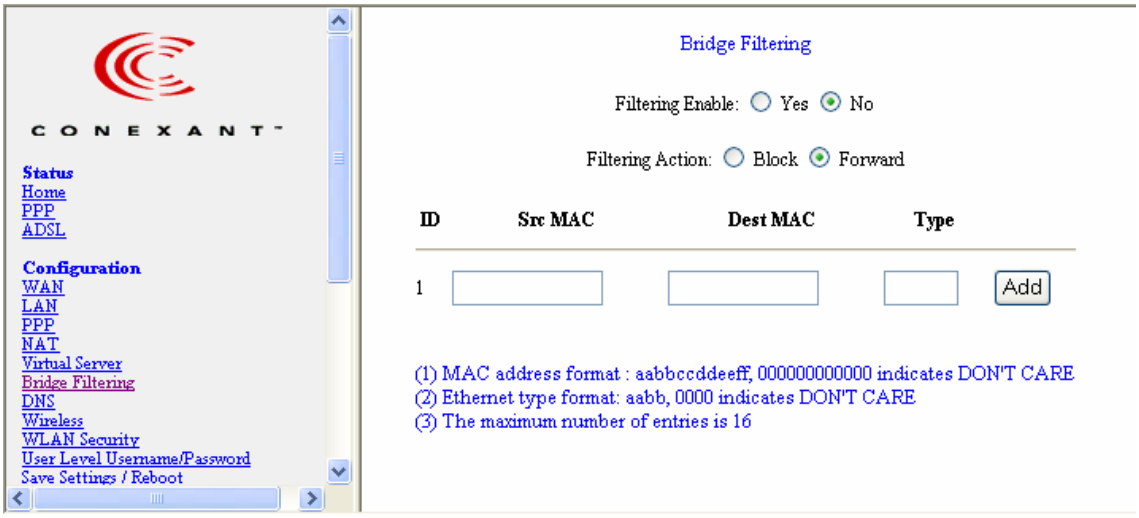
If you want to disable port 23 with both TCP and UDP protocols:

ID	Public Port	Private Port	Port Type	Host IP Address
1	23	23	choose TCP	192.168.2.101
2	23	23	choose UDP	192.168.2.101

Once done, save it and reboot your modem.

Bridge filtering

Bridge Filtering allows packets to be forwarded or blocked, depending on the MAC address The **Bridge Filtering** configuration page allows users to set the configuration of IP filtering.

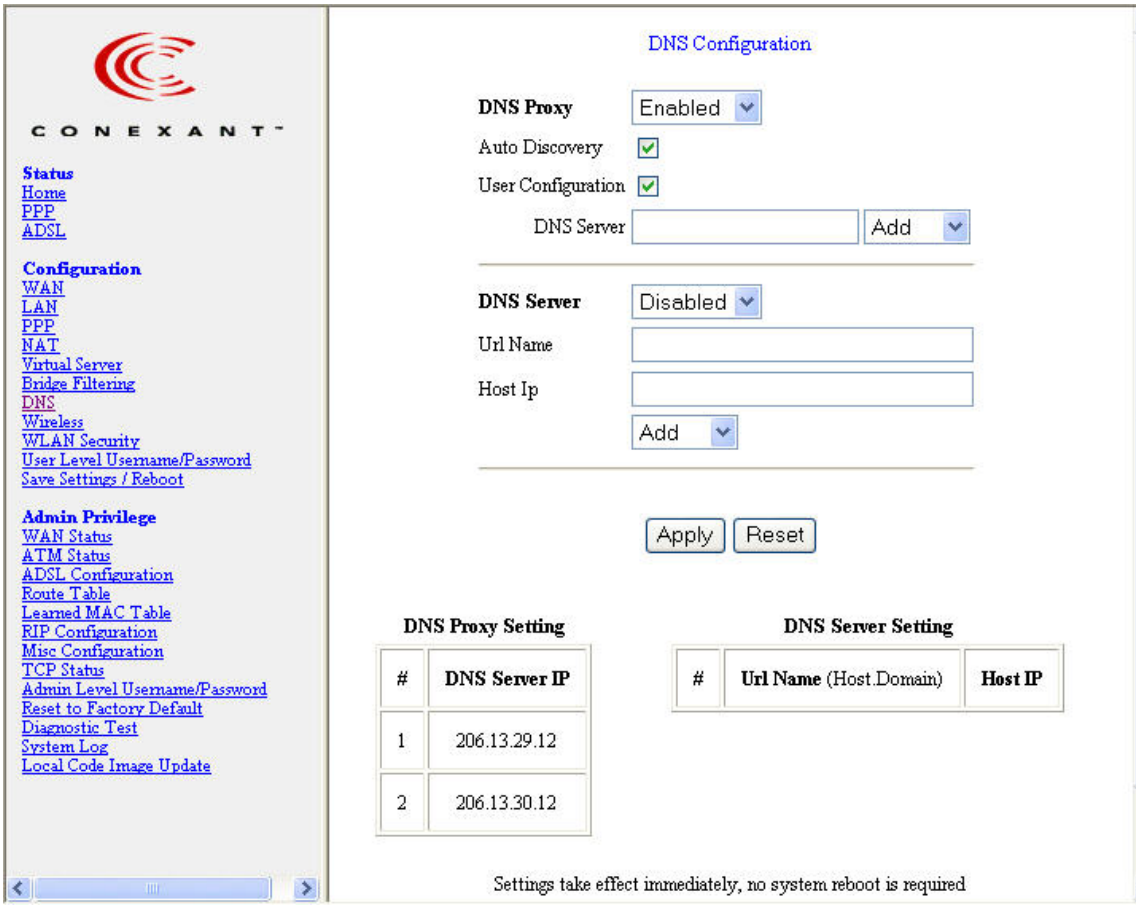


- **Source MAC:** When the bridge filtering is enabled, enter the **Source MAC address**, select **Block** and click **Add**. Then all incoming WAN and LAN Ethernet packets matched with this source MAC address will be filtered out. If the **Forward** is selected, then the packets will be forwarded to the destination PC.
- **Destination MAC:** When the bridge filtering is enabled, enter **the Destination MAC address**, select **Block** and click **Add**. Then all incoming WAN and LAN Ethernet packets matched with this destination MAC address will be filtered out. If the **Forward** is selected, then the packets will be forwarded to the destination PC.
- **Type:** Enter the hexadecimal number for the Ethernet type field in Ethernet_II packets. For example, 0800 is for IP protocol.
- **Block:** When block is selected, everything from the **Source MAC** with destination **Destination MAC** will be blocked.
- **Forward:** When forward is selected, everything from the **Source MAC** will be forwarded to the **Destination MAC**.

DNS Configuration

Domain Name Service (DNS) is a service used on the Internet for resolving fully qualified domain names (FQDN) to their Internal Protocol (IP) address. You can type the preferred DNS server IP address, Alternative DNS server IP address that provided by ISP or automatically assigned by ISP. Click **Submit** and **Save Settings** to save your setting.

The **DNS Configuration** page allows users to set the configuration of DNS proxy.



The firmware supports the DNS proxy function. For the DHCP requests from local PCs, the DHCP server will set the LAN port IP as the default DNS server. Thus, all DNS query messages will come into LAN port first. The DNS proxy on the ADSL modem recorded the available DNS servers, and forward DNS query messages to one of DNS server.

There are four DNS proxy modes available:

- **Disable DNS Proxy:** The LAN port does not process the DNS query message. For the DHCP requests from local PCs, the DHCP server will set the user-configured preferred DNS sever or alternate DNS server whichever is available as the DNS server. Then all DNS query messages will be directly sent to the DNS servers.

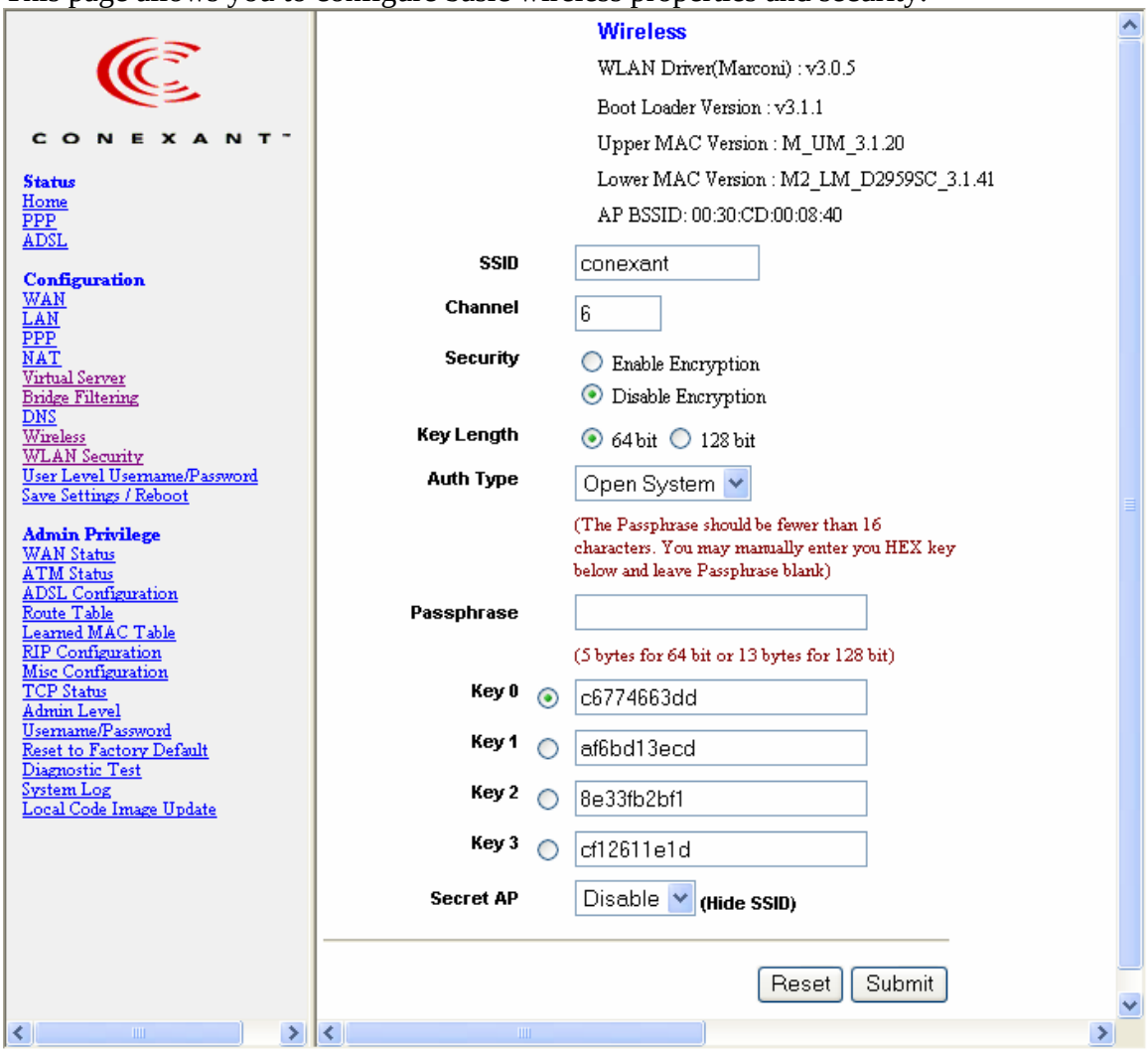
- **Use Auto Discovered DNS Servers Only:** The DNS proxy will store the DNS server IP addresses obtained from DHCP client or PPP into the table. And all DNS query messages will be sent to one of the dynamically obtained DNS servers.

- **Use User Configured DNS Servers Only:** The DNS proxy will use the user-configured preferred DNS server and alternate DNS server. And all DNS query message will be sent to one of DNS servers.

- **Auto Discovery + User Configured:** The DNS proxy's table has all the IP addresses of dynamically obtained and user configured DNS servers.

Wireless

This page allows you to configure basic wireless properties and security.



- **SSID :** An **SSID** (acronym for Service Set Identifier) is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 31 characters.

- **Channel:** Select the appropriate channel to correspond with your network settings, between 1 and 14. All access points and wireless PC adaptors must share the same channel to interoperate.

  Range is for Channel field is 1 – 14, default is 6. If any number greater than 14 is entered, the field will default to the value 11.

- **Security:** The ADSL Bridge/Router provides a security encryption tool known as WEP (Wired Equivalent Privacy). WEP is designed to provide security and privacy equivalent to that found in a wired network. This is done by encrypting the data packets sent between client and host with an encryption key. Both the client (PC) and the host (access point/router) must have the same WEP key in order to communicate. The available WEP settings are 64 bit and 128 bit. The higher the bit value on the encryption, the more secure the data transmission. Select **Enable Encryption** to activate this feature.

- **Key Length:** Choose between 64 bit (default) and 128 bit. 128 bit offers more security, but at the cost of slower packet processing.
  Key 0-3: You are able to enter 4 encryption keys, only one of which is enabled at any given time. All devices on the network must share the selected key in order to communicate with the ADSL Bridge/Router AP. The key length for 64 bit is 10 hexadecimal characters and the key length for 128 bit is 26 hexadecimal characters.
  Note: If you have the WLAN Security (see next section) enabled, always choose WEP Key ID 2. This will allow the 802.1x client and non-802.1x client to work simultaneously in the 802.1x WLAN security Method.

- **Auth Mode:** Select Open System or Share Key to set the authentications the Access Point recognizes.

  - Open System: This default setting allows any device, regardless of its WEP keys, to authenticate and then attempt to associate.

  - Shared Key: This setting tells the Access Point to send a plain-test, shared key query to any device attempting or associate with the Access Point. This query may leave the Access Point open to a known-text attack from intruders and is therefore not as secure as the Open System setting.

  - Both: allow both Open System and Shared Key modes

- **Secret AP**: enable or disable AP broadcast to show or hide AP. When AP broadcast is disabled, your AP would not be shown on most wireless scanners such as NetStumbler.

Click the **"Submit"** and **"Save Setting"** buttons once confirm your setting or configuration and reboot the device in order to activate the setting.

Wireless LAN (WLAN) Security

WiFi Protected Access (WPA) security certification is a partial snapshot of 802.11i. It includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. The combination of these two mechanisms provides dynamic key encryption and mutual authentication,

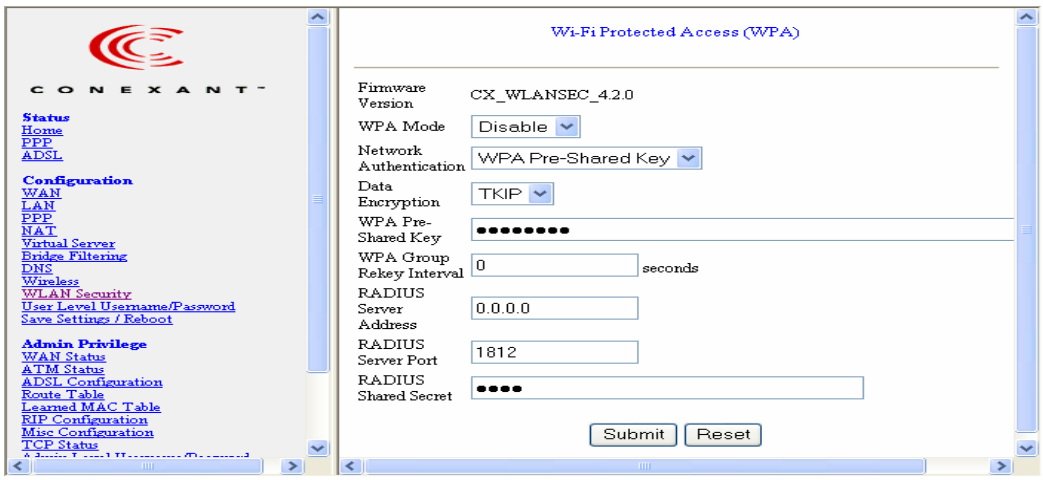
With WPA, you can connect this modem with RADIUS server to perform 802.1x for authentication. 802.1x is an IEEE standard that enables authentication and key management for LANs. Although originally designed as a port authentication scheme for wired networks, it has recently been applied to address some of the security issues surrounding wireless LANs.

The use of IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as Kerberos, token cards, one-time passwords, certificates, and public key authentication. Port security provides another means to ensure that only authorized users are on the network by limiting access based on MAC addresses. For authentication of users with a RADIUS server, 802.1x provides port-level security.

Such RADIUS service allows you to authenticate clients with **802.1x** authentication.

It requires three roles in the authentication process: that of an supplicant, an authenticator and an authentication server.

- **Supplicant**: WLAN users run an 802.1x client which supports a strong EAP authentication method such as EAP-TTLS
- **Authenticator**: 802.1x compliant access points. See Appendix D as an example for how to setup Cisco Aironet 350 as 802.1x AP.
- **Authentication server**: such as RADIUS server which supports a strong EAP authentication methods such as EAP-TTLS. Examples are Windows 2000 Server with IAS on, or FreeRadius server.



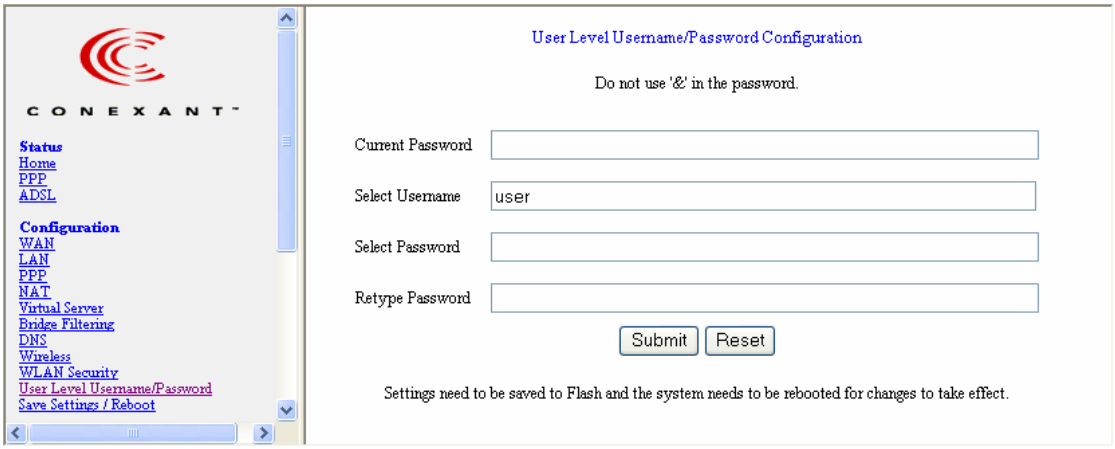
- **Firmware Version:** This is the version of the Wireless Security firmware.
- **WPA Mode:** This field allows you to enable/disable WLAN Security.
- **Network Authentication:** There are two available methods of WLAN Security:
    - **WPA RADIUS:** This option uses 802.1X for authentication with RADIUS server while using TKIP encryption.
    - **WPA Pre-Shared Key:** This option uses a pre-shared key (psk) for authentication while using TKIP encryption.
- **Data Encryption**: support TKIP.
- **WPA Pre-Shared Key:** This is the pre-shared key for use in WPA PSK security method.
- **WPA Group ReKey Interval (sec):** This is the time-out value for the WPA Group Key.

Note: With WLAN Security enabled, select "Enable Encryption" and choose WEP Key ID 2 on the Wireless Page (see previous section). This will allow the 802.1x client and non-802.1x client to work simultaneously in the 802.1x WLAN security Method.

- **RADIUS Server Address:** This is the IP address of the RADIUS server.
- **RADIUS Server Port:** This is the UDP port of the RADIUS server. Default to 1812
- **RADIUS Shared Secret:** This is the password shared between an 802.11 access point and the RADIUS server.

User Level Username/Password

This page allows the **user** or **admin** to set the password for the user account.



The User Password can be up to 65 characters (excluding '&').
Note: User Account cannot be used to access FTP server.

Save Settings / Reboot

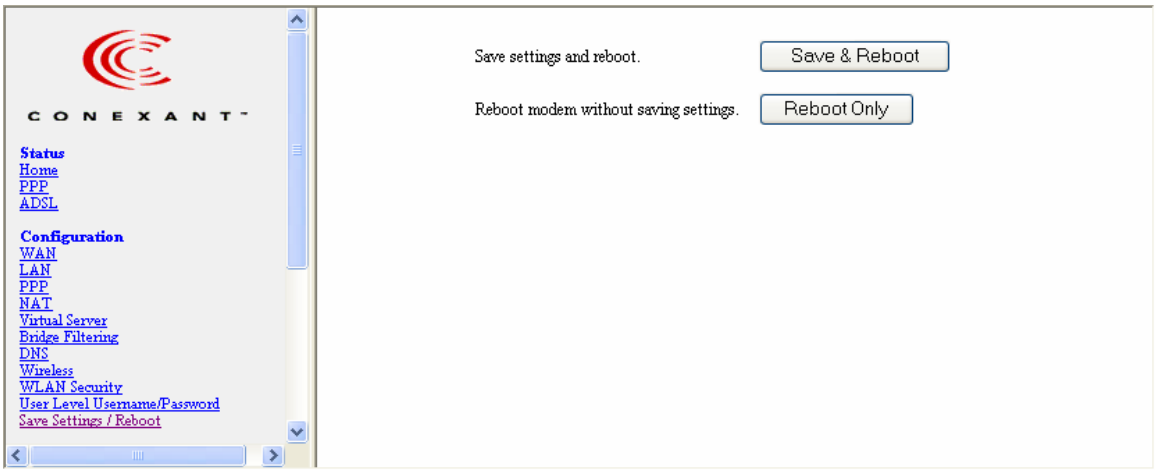
The **Save Settings** page allows users to save the new configuration to the flash and reboot the system.

When you change all setting, you must click **save settings** and click **submit**. The Router will save settings and software reset router for about 20 seconds.

- **Save & Reboot:** Click this to apply all changes.
- **Reboot Only:** Do this to discard all changes since last save.

After either one of these buttons are clicked, the ADSL Bridge/Router will do the following:

- **Save & Reboot:** Two pages will appear after pressing this button. The first one states: “Your settings are being saved and the modem being rebooted. Save and reboot in progress, please wait….” Followed by “Your settings have been saved and the modem has rebooted. Done”
- **Reboot Only:** Two pages will appear after pressing this button. The first one states: “The modem is being rebooted. Reboot in progress, please wait….” Followed by “The modem is being rebooted. Done.”

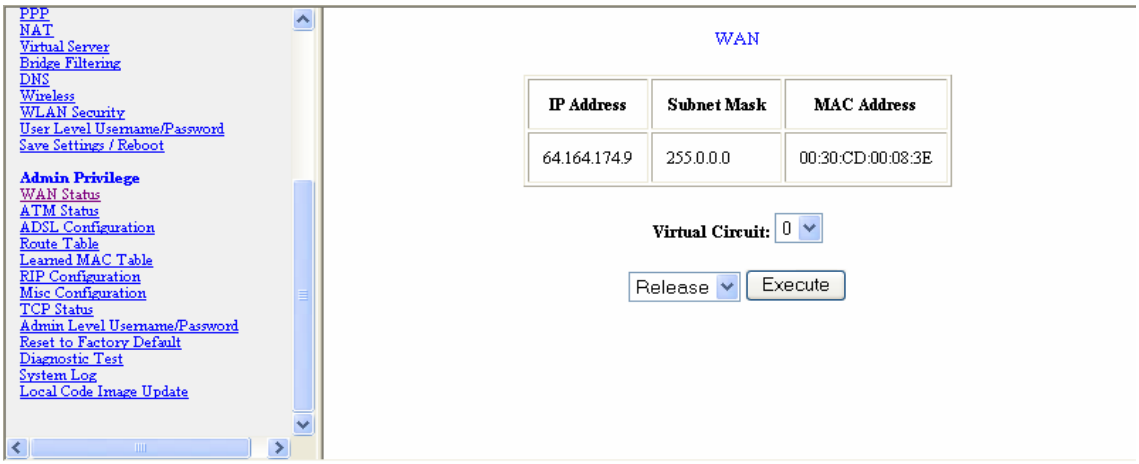


CHAPTER 7 ADMIN PRIVILEGE

The links under **Admin Privilege** are only accessible when user is logged in as **Admin**. Regular user account does not have authorization to view or alter the content on the pages in the **Admin Privilege** section.

WAN Status

The **WAN Status** page shows the information and status of WAN PVCs.

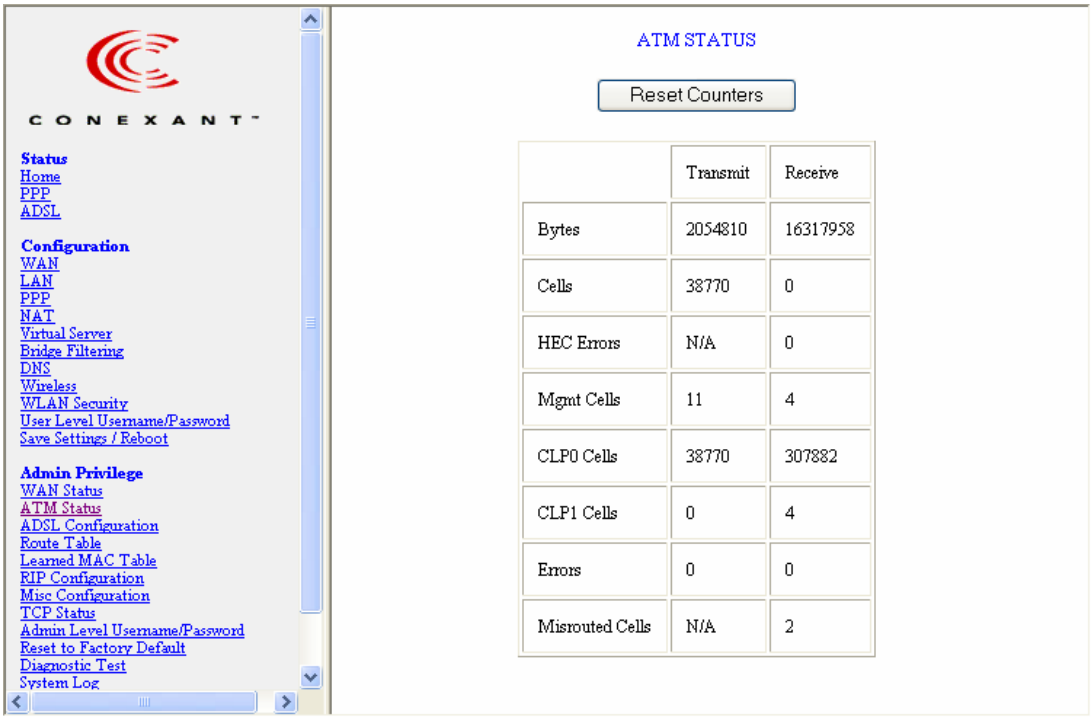


WAN: This field displays the IP address, Subnet Mask and MAC address for the WAN (ADSL) interface. Use the Virtual Circuit selection to select different PVCs for status display.
Virtual Circuit: Select the Virtual Circuit that you want to release/renew, select the appropriate option on the menu dropdown and click **Execute**.

ATM Status

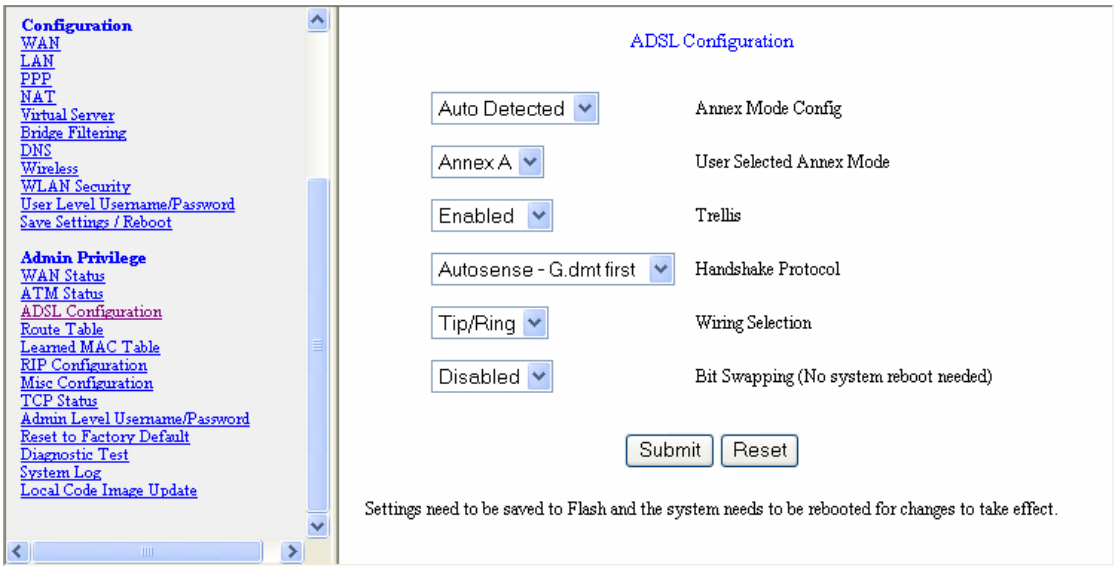
The **ATM Status** page shows all the statistics information of ATM cells. This page contains information that is dynamic and will refresh every 2 seconds.

Reset Counters: This button allows user to reset the ATM Status counter.
ATM Status Fields: Tx Bytes, Rx Bytes, Tx Cells, Rx Cells, Rx HEC Errors, Tx Mgmt Cells, Tx CLP0 Cells, Rx CLP0 Cells, Tx CLP1 Cells, Rx CLP1 Cells, Rx Errors, Tx Errors, and Rx Misrouted Cells.



ADSL Configuration

The **ADSL Configuration** page allows you to set the configuration for ADSL protocols.

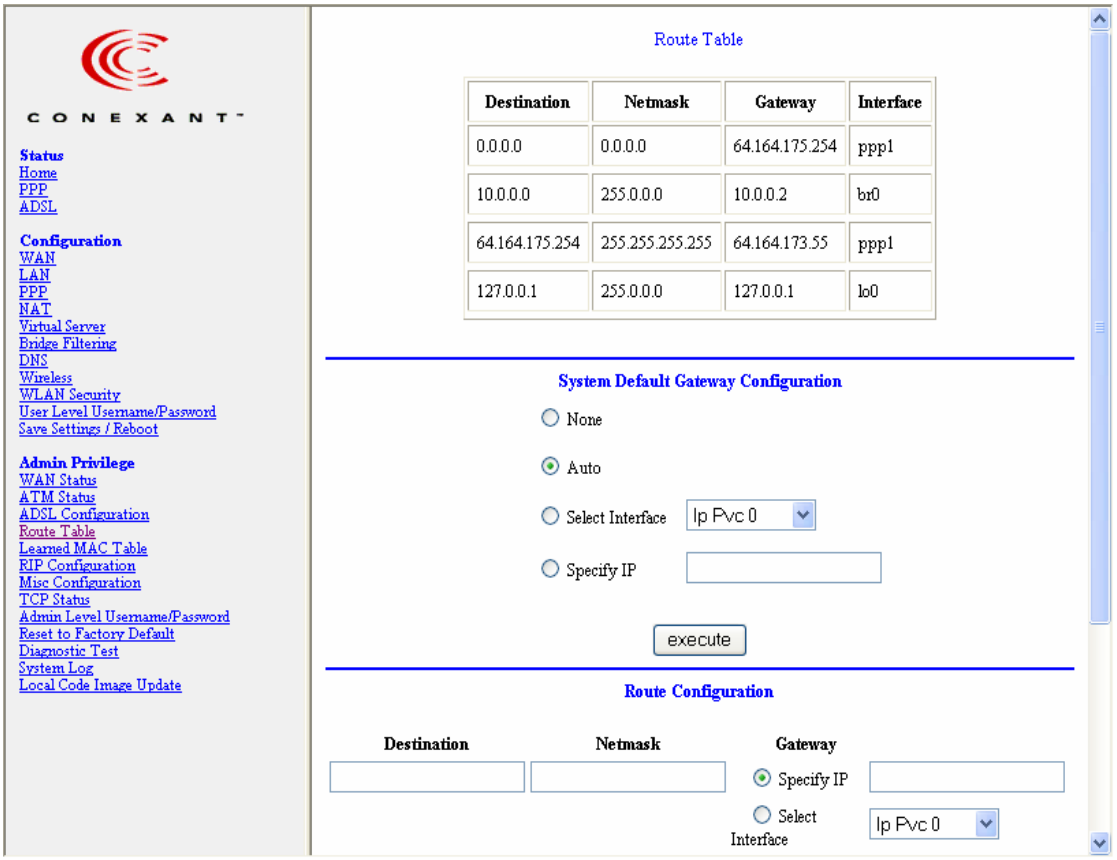


Annex Mode Config: This allows you to manually configure the ADSL Bridge/Router for Annex A or Annex B mode by selecting User Configured and choosing the Annex Mode in the next field.

User Selected Annex Mode: This allows you to select from Annex A and Annex B.
Trellis: Trellis Code is an advanced method of FEC (Forward Error Correction). This field allows you to enable or disable the Trellis Code. By default, it is always enabled.
Handshake Protocol: This field allows you to select from the following ADSL handshake protocols: Autosense – G.dmt first (default), Autosense – T1.413 first, G.dmt/G.lite, T1.413, G.dmt, and G.lite.
Wiring Selection: This field allows you to enter the wiring selection for the RJ-11. Tip/Ring is the default for the ADSL Bridge/Router without the inner/outer pair relay. Available types are Auto, Tip/Ring (default), and A/A1, where Tip/Ring is the inner-most pair of wires on the RJ11 and A/A1 is the second inner-most pair.
Bit Swapping: This field allows you to enable or disable the upstream bit swapping. Bit Swapping is disabled by default.

Route Table

The **Route Table** page displays the routing table and allows you to manually enter a routing entry. The routing table will display the routing status of Destination, Netmask, Gateway, and Interface. The interface br0 indicates the USB interface; lo0 indicates the loopback interface; ppp1 indicates the PPP interface. The Gateway is the learned Gateway.



• The Gateway field of the static route entry allows users to either enter a Gateway IP address or select a Network Interface.

• All user-defined routes retained in the CPE memory, regardless if they are already in the
Routing Table, are displayed on the same Route Table page.

• All user defined route entries kept in the CPE memory during run time are saved to flash
when the user chooses to save and reboot the CPE. When the CPE restarts, it reloads all saved user-defined routes to the CPE memory and tries to apply to the system.

• A user-defined route entry is added to the Routing Table whenever the system provides an environment that makes the route entry applicable. It is removed from the Routing Table whenever the route entry becomes not applicable. e.g. If the route entry's Gateway is associated with a dynamic Network Interface but the connection is not established, then the route entry does not appear in the Routing Table. When that interface comes up later, the route entry is then added.

• If the selected Network Interface is static or dynamic and the connection is already up, then the route entry appears in the Routing Table immediately. If there is a Gateway associated with the selected Network Interface, then that Gateway's IP address appears in the Gateway field of the route entry.
If the selected Network Interface is dynamic but the connection is not established, then the route entry does not appear in the Routing Table. When the interface comes up later, the route entry is then added.

System Default Gateway Configuration

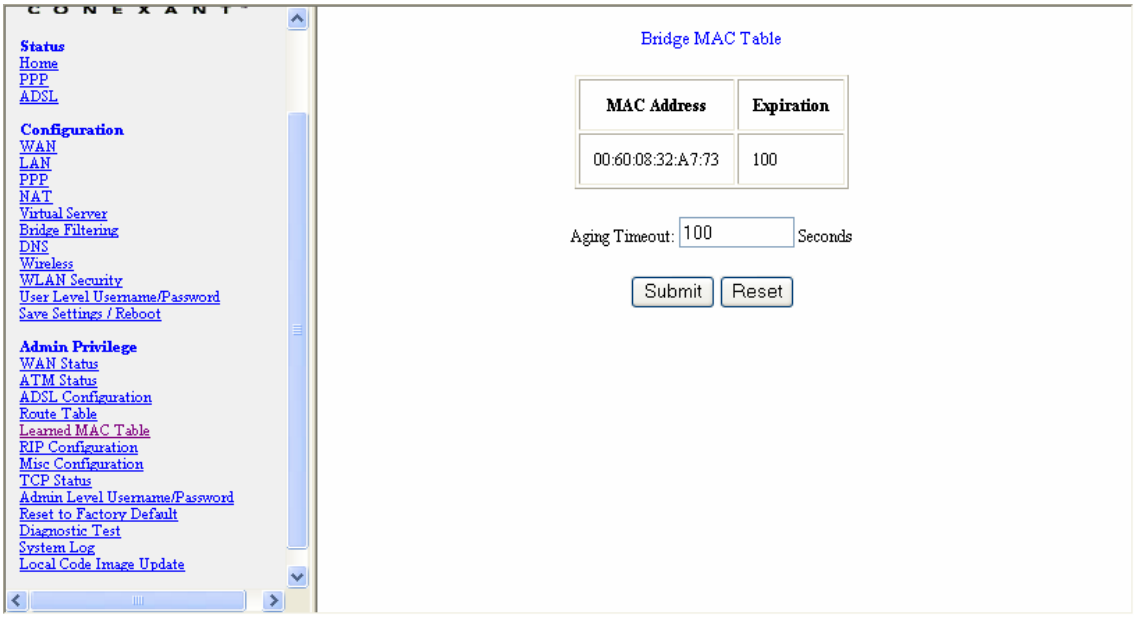
The system-wide Default Gateway provides three options: Auto (default), User-selected Network Interface, and None.
None: This field allows you to choose to have no Default Gateway in the CPE
Auto: This field allows you to enable the Bridge/Router to automatically decide the Default Gateway.
User-selected Network Interface: This field allows you to select a Network Interface from a list (PVCs, PPP Sessions, USB and LAN). This option allows you to associate the system-wide Default Gateway to a Network Interface, static or dynamic, and provides a way to fix the Default Gateway to a dynamic Network Interface before the interface is established.
The options for this field are IP PVC0 ... IP PVC7, IP Ethernet 0, IP BridgeMux0, and any PPP session that was created by the user.
Specify IP: This field allows you to specify the IP address of the default gateway.

Route Configuration

Destination: This field allows you to enter the remote network or host IP address for the static routing.
Netmask: This field allows you to enter the Subnet Mask for the static routing.
Gateway: This field allows you to enter the IP address of the gateway device that allows the router to contact the remote network or the host for Specified IP or select an Interface for the Gateway.
Manually Configured Routes: This field displays the static route entries entered by the user.

Learned MAC Table

Network bridges operate at the physical network layer. The purpose of a bridge is to connect two or more networks and enable packet sharing between them. Bridges are different from routers because they forward packets based on physical addresses, whereas routers use IP address to forward packets. Bridges must learn all the physical (MAC) addresses of the devices so it can forward the packets reliably. The purpose of the **Learned MAC Table** is to store and display these bridge-recognized MAC addresses. The **Learned MAC Table** page shows the current learned Bridge MAC table. This page contains information that is dynamic and will refresh every 8 seconds.
Aging Timeout: This field allows you to enter the update period for the MAC table. Have this number lower if you want a more frequent refresh rate.
Range for Aging Timeout field is 0 – 32767, default is 100.



RIP Configuration

RIP (Routing Information Protocol) is a management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge. There are several components to RIP, including the authenticator, supplier, and listener.
Authenticator: Authentication is only available for RIPv2. When it is disabled, RIPv2 messages containing authentication entries are discarded. When it is enabled, all RIPv2 messages must have proper authentication entries, and all RIPv2 messages without verified authentication entries and all RIPv1 messages are automatically rejected.
Supplier: The RIP Supplier has two functions:

• It transmits route updates over every RIP Supplier interface at the interval specified by **Supply Interval** (see below).

• It transmits route updates in response to specific requests from other routers.

Listener: The RIP Listener listens and processes all RIP messages it receives from other RIP routers and updates the host routing tables accordingly. The RIP Listener is always enabled when RIP is enabled. By default, RIP is disabled.
The announcement messages RIP sends are based on two configuration parameters: RIP Version number and Multicast:

Version	Multicast	Announcements Sent
1	OFF	V1
2	ON	V1
2	OFF	V2-BC
2	ON	V2-MC

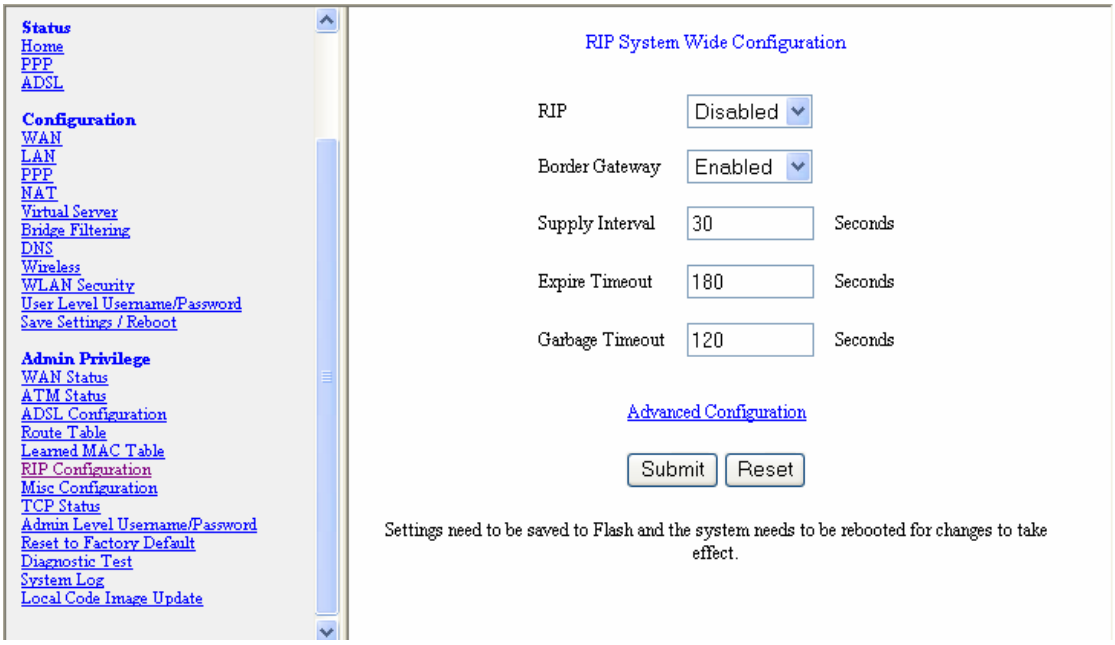
The RIP messages that can be received and processed are based on two configuration parameters: RIP Version number and Multicast:

Version	Multicast	RIP Messages Received
1	OFF	V1
2	ON	V1
2	OFF	V1 & V2-BC
2	ON	V2-BC VC-MC

The **RIP Configuration** page allows you to set the configuration for the system wide configuration of RIP. The actual RIP configuration is in the RIP Per Interface Configuration.

RIP: This field allows you to Enable or Disable the RIP session. The resulting RIP session will monitor all network interfaces that are currently available for messages from other RIP routers. RIP is disabled by default.

Border Gateway: RIP implements Border Gateway as specified in RFC 1058 and RFC 1723. This limits all subnet routes and host routes to routers within that same network. Updates sent outside that network will only include a single entry representing the entire network, including all subnets and host-specific routes. The Border Gateway is enabled by default.



Supplier Interval: This field allows you to enter the Supplier Interval timer in seconds. This timer specifies how often the RIP sends announcements as a RIP Supplier.
Range for Supplier Interval field is 0 – 2147483647, default value is 30.
Expire Timeout: This field allows you to enter the Expire Timeout in seconds. This timer specifies the expiration time of a route. When a route has not been updated for more than the "expire" period of time, it is removed from the Route Table. This route is then invalidated and remains in the internal RIP Route Table. It will be included in the RIP announcements to let other routers know the changes.
Range for Expire Timeout field is 0 – 2147483647, default is 180.
Garbage Timeout: This field allows you to enter the Garbage timer in seconds. This timer specifies how long the expired and invalidated routes are kept in the Internal RIP Route Table before they are removed from it.
Range for Garbage Timeout field is 0 – 2147483647, default is 120.

RIP Per Interface Configuration

The RIP Per Interface Configuration page allows you to set the configuration for each Interface (PVCs, PPP Sessions, USB and LAN).

Interface: This field allows you to choose the Interface (PVCs, PPP Sessions, USB and LAN), for the RIP to be configured. The available selections are: IP Ethernet 0, IP USB 0, IP PVC0...IP PVC7, IP BridgeMux 0, and any PPP user defined sessions maximum of 16):

Enable: This field allows you to Enable (Yes) or Disable (No) the specified interface for RIP.

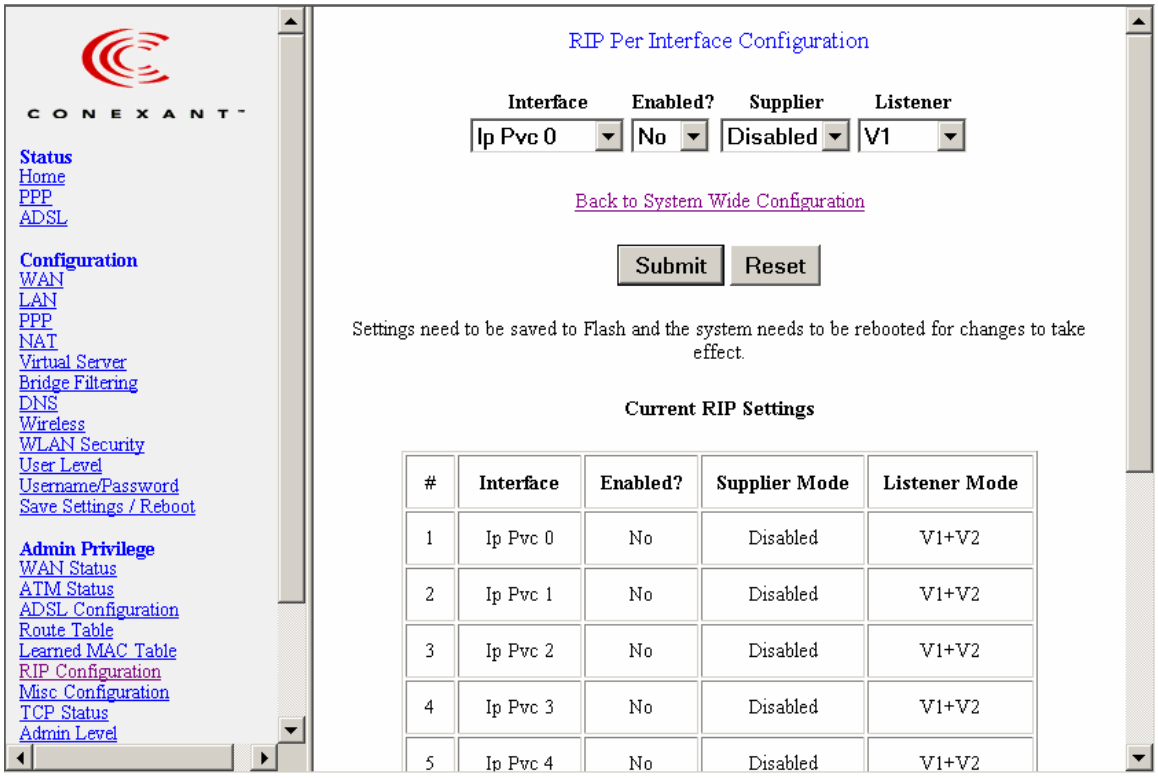
Supplier: This field allows you to select the Supplier Mode (RIP Transmit).

- Disabled: The supplier transmit is disabled.
- V1 BC: The supplier transmits in RIPv1 Broadcast.
- V2 BC: The supplier transmits in RIPv2 Broadcast.
- V2 MC: The supplier transmits in RIPv2 Multicast.

Listener: This field allows you to select the Listener Mode (RIP Receive)

- V1: The listener receives the RIPv1 only.
- V2: The listener receives the RIPv2 only.
- V1+V2: This listener receives the both RIPv1 and RIPv2.

Current RIP Settings: This field displays the each interface's RIP status.

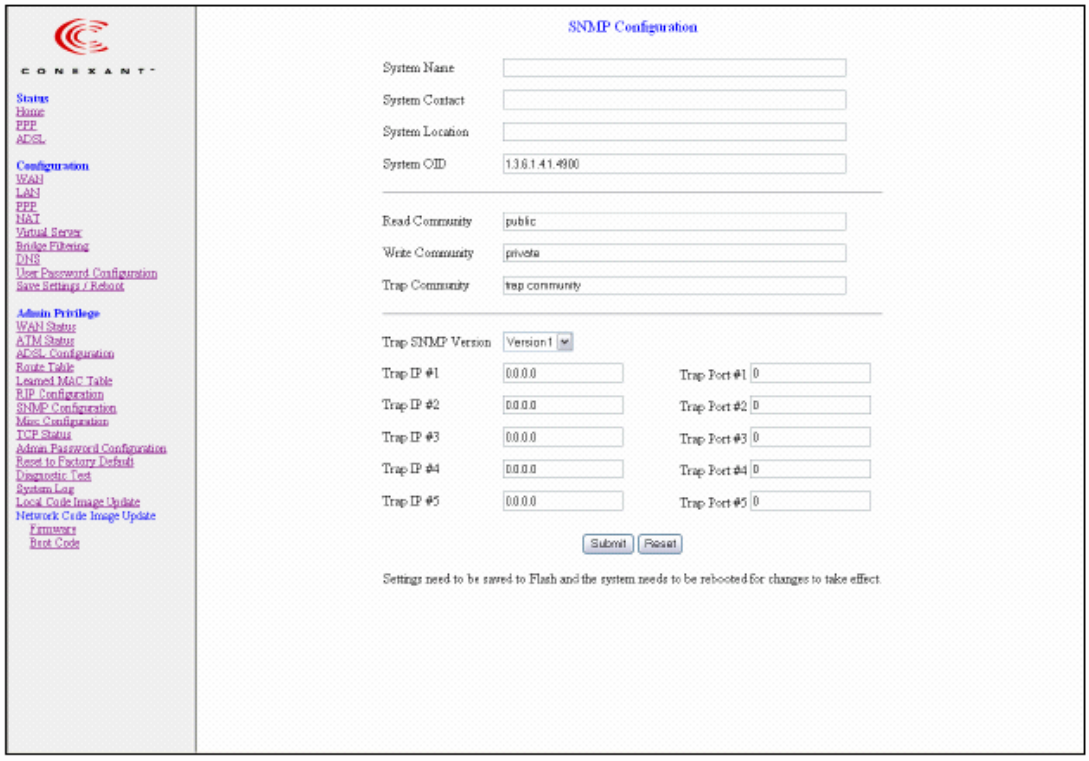


SNMP Configuration

Simple Network Management Protocol (SNMP) is an optional feature that may or may not be supported by your ADSL Bridge/Router.

SNMP is an application layer protocol that is used for managing networks. SNMP is an optional feature that may or may not be in the specific firmware that you are working with. There are several components that make up the SNMP structure, including agents, network management stations (NMS), network management protocols, and a management information base (MIB). An SNMP agent is a node that resides on the network, typically a computer or a router. The SNMP agent is controlled and configured by the NMS by sending SNMP messages between one another. SNMP agents are logged and identified in a Management Information Base (MIB), in which they are identified by an object identifier (OID).

One feature of SNMP is SNMP traps. SNMP traps are used to notify network managers of significant events that have taken place in the network. These traps are sent to the SNMP NMS (NMS Server located at Trap IP) through the specified Ports.



SNMP System Identification: The System Name, System Contact, System Location, and System OID are provided to identify the SNMP NMS. The System OID is the ID number placed in all Trap reports.

The System Name, System Contact, and System Location can be up to 127 characters. Default value for System OID is 1.3.6.1.4.1.4900.

Read Community: This is the password to access public information.
The Read Community can be up to 127 characters. Default is "public."

Write Community: This is the password to access private information.
The Write Community can be up to 127 characters. Default is "private."

Trap Community: This is the password to access and view SNMP traps.
The Trap Community can be up to 127 characters. Default is "trap community."

Trap SNMP Version: Select from Version 1 or Version 2. Default is Version 1.

Trap IP: This is the IP address to which SNMP traps are sent. There can be up to 5 different SNMP trap destination IP addresses.

Trap Port: This is the corresponding port for the SNMP trap (see **Trap IP** above). Range for Trap Port field is 0 – 32767.

Miscellaneous Configuration

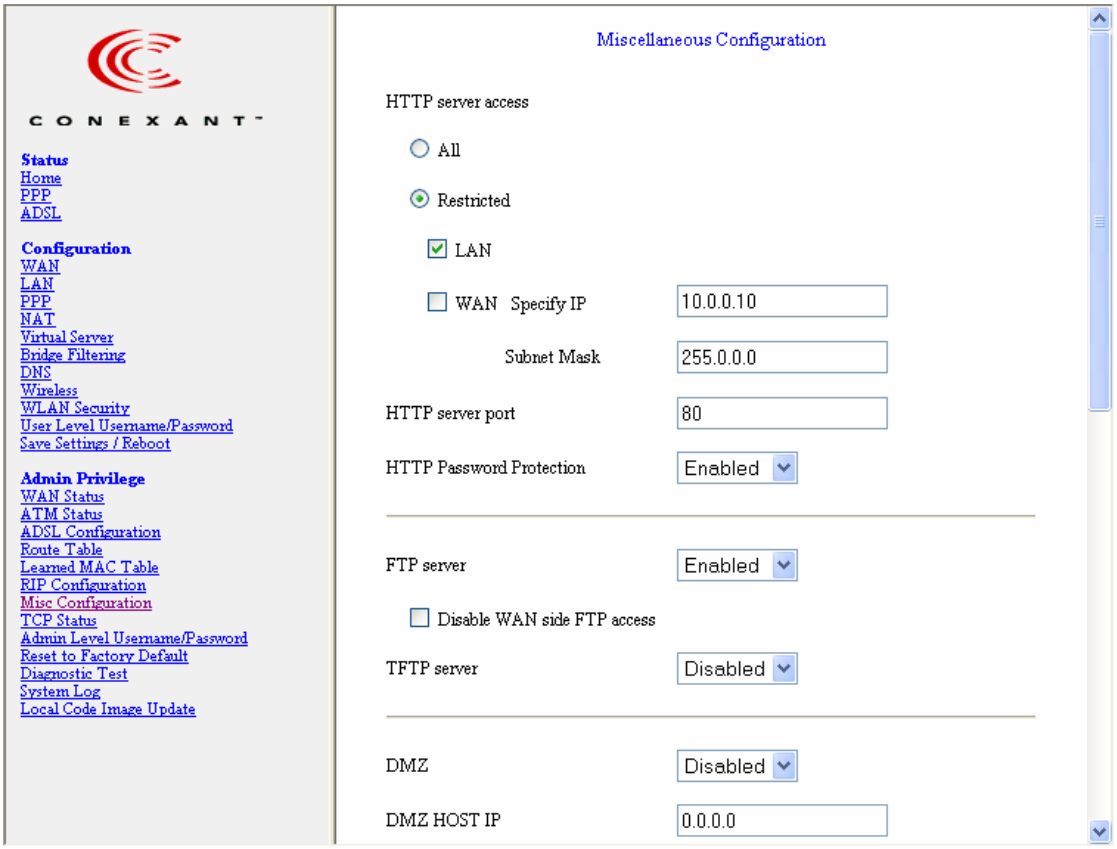
The **Miscellaneous Configuration** page allows you to set miscellaneous configurations for the following: HTTP, FTP, TFTP, DMZ, Command Line Interface, DHCP, PPP, IGMP, and SNTP.

HTTP Server Access: This field allows you to configure where these Web pages can be accessed from.

• **All:** When this field is checked, it allows both WAN and LAN access to the Web pages. This is the system default.

• **Restricted LAN:** This field allows the Web pages access from LAN side.

• **Restricted WAN Specified IP & Subnet Mask:** This field allows the Web access from WAN side with a specify IP and subnet mask.



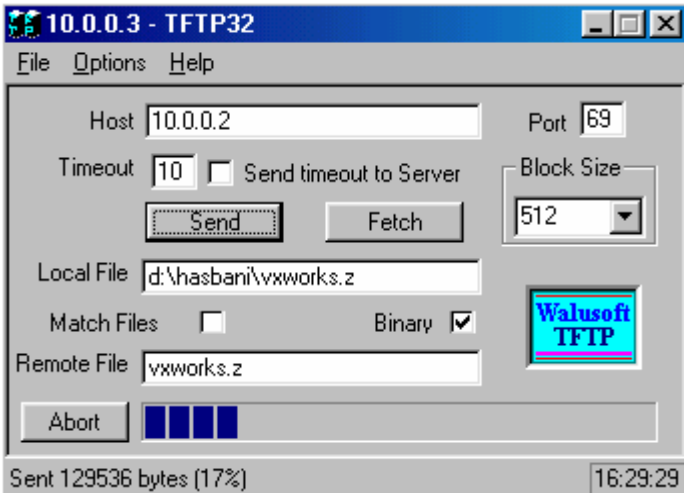
HTTP Server Port: This field allows you to specify the port of the Web access. . For example, when it is changed to 8080, the HTTP server address for the LAN side is **http://10.0.0.2:8080**. Range for HTTP Server port is 0 – 32767, default value is 80.

FTP server: This field allows you to enable or disable the FTP server connection. System default is Enabled.

• **Disable WAN side FTP access:** This will disable WAN side access to the FTP server, default is Disabled.

TFTP server: This field allows you to enable or disable the TFTP connection. System default is Disabled.

An example for the TFTP client updating the vxworks.z product image code is:



DMZ: A DMZ (De-Militarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security. When there is a suspected packet coming from WAN, the firewall will forward this packet to the DMZ host.

DMZ Host IP: The IP address of the DMZ host viewable at the WAN (external) side.

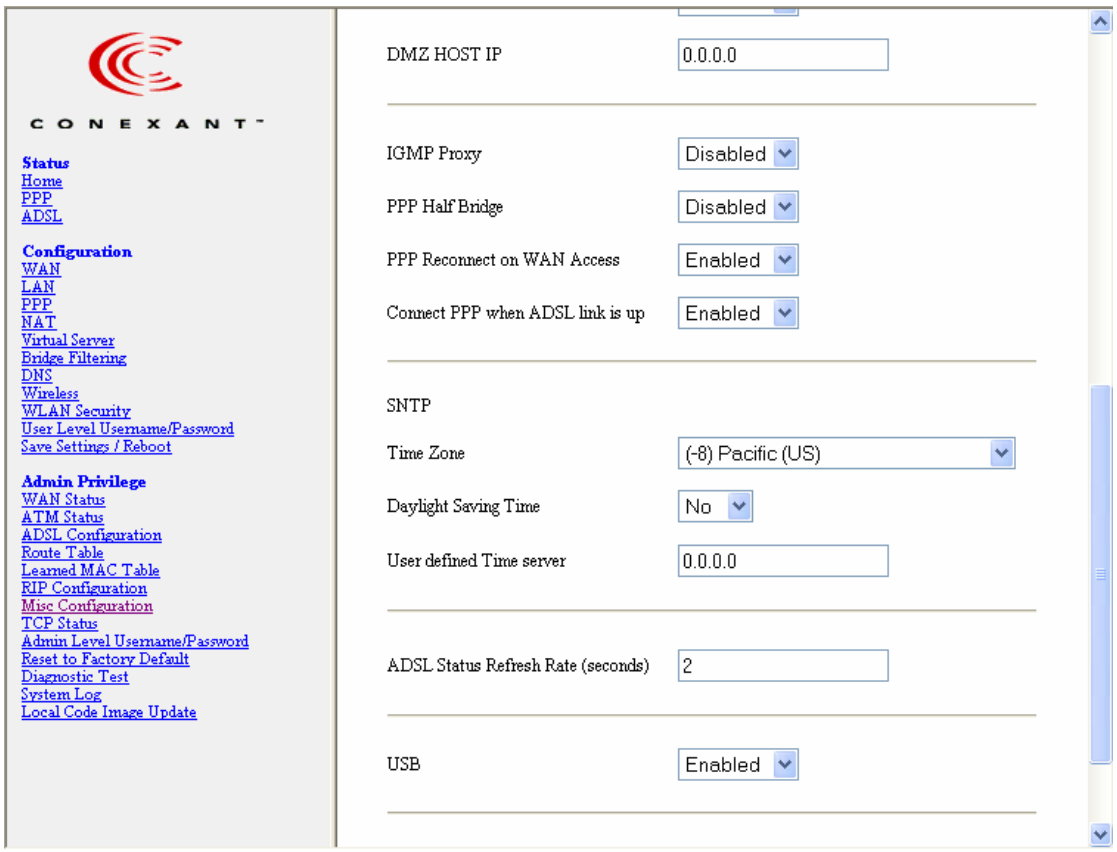
DHCP

• **NONE:** This will disable the DHCP server. Note that this setting will override the DHCP Server Enable/Disable on the LAN configuration page.

• **DHCP Server** (default)**:** Select this to activate the DHCP server.

• **DHCP Relay:** If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please disable the NAT to run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

DHCP Relay Target IP: If DHCP Relay is enabled, DHCP requests are relayed to DHCP Target IP on the WAN side.



IGMP Proxy: This is the global setting for IGMP Proxy. If it is enabled, then the enabled IGMP Proxy on WAN PVCs will be working. Otherwise, no WAN PVC can have IGMP Proxy working on it. System default is Disabled.

PPP Half Bridge: When PPP Half Bridge is enabled, only one PC is able to access the Internet, and the DHCP server will duplicate the WAN IP address from the ISP to the local client PC. Only the PC with the WAN IP address can access the Internet. System default is Disabled.

PPP reconnect on WAN access: If enabled, the PPP session will automatically establish a connection when a packet tries to access the WAN. System default is Enabled.

Connect PPP when ADSL link is up: If this option is enabled, the bridge/router will connect the PPP session whenever an ADSL connection is established. If this option is disabled, the PPP session will not connect whenever the ADSL Showtime is reached. System default is Enabled.
Note: For more information/clarification, please refer to Section 4.4: PPP Configuration.
SNTP: Simple Network Time Protocol is a efficient method of obtaining the time from a Time Server.

Time Zone: This specifies the time zone (geographical location).

Daylight Saving Time: You can select yes to activate Daylight Savings Time.

User defined Time server: This is the time server from which the ADSL Bridge/Router retrieves the time.

TCP Status

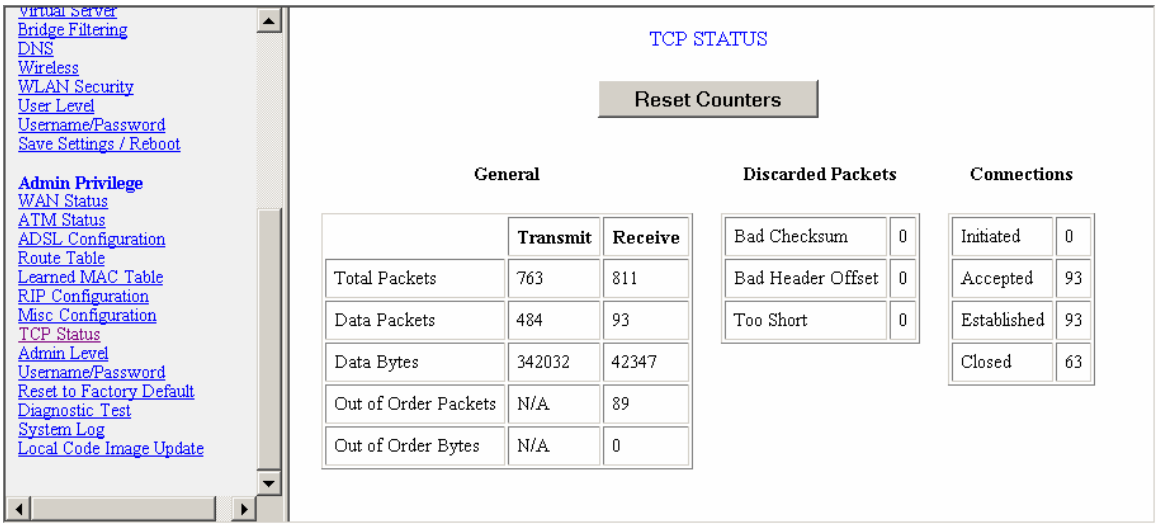
The **TCP Status** page shows the statistics for all TCP connections. This page contains information that is dynamic and will refresh every 2 seconds.

Reset Counters: This button allows user to reset the TCP Status counter.

General: Total Packets, Data Packets, Data Bytes, Out of Order Packets, Out of Order Bytes

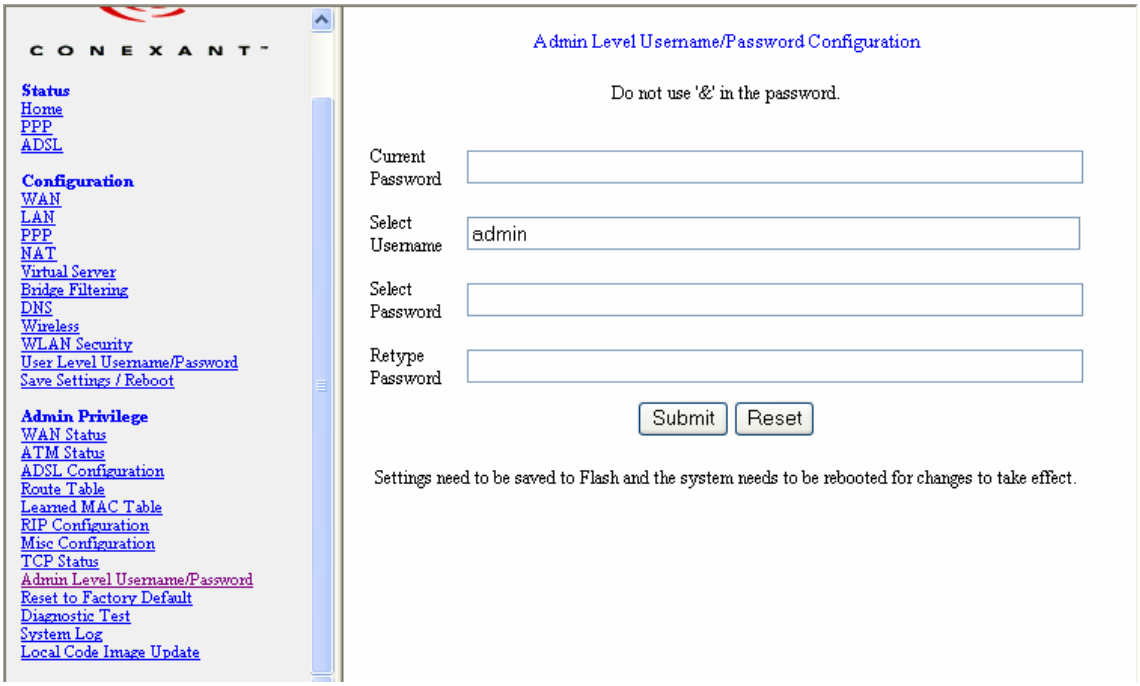
Discarded Packets: Bad Checksum, Bad Offset Header, Too Short

Connections: Initiated, Accepted, Established, Closed.



Admin Password Configuration

The **Admin Password Configuration** page allows you to set the password for **administrator.**



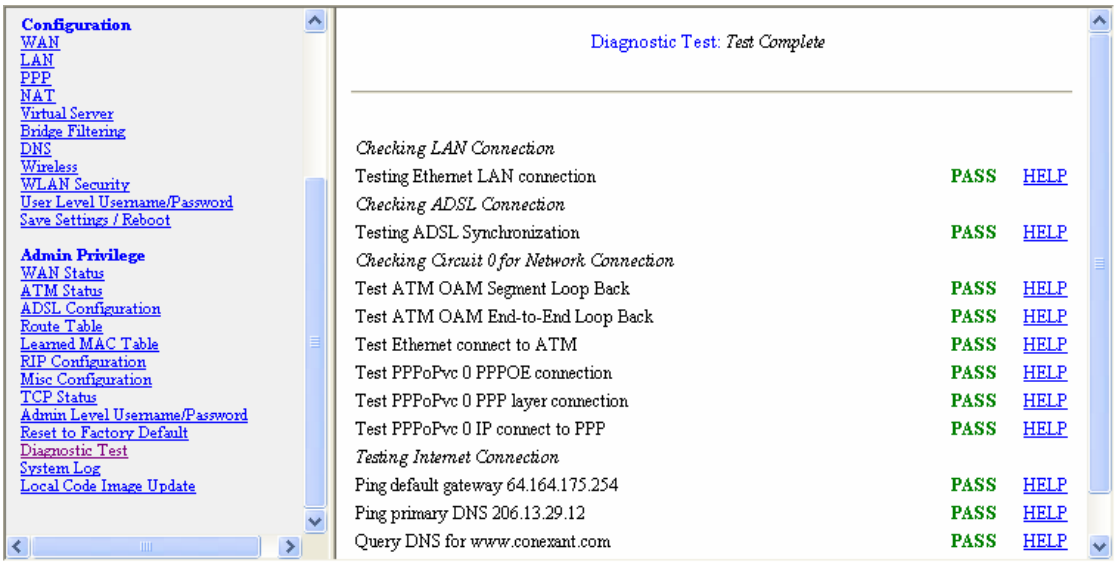
The Admin password is same as the FTP password, so it must have at least 8-characters for the FTP to work. The Admin password can be up to 65 characters (excluding '&').

Reset to Factory Default

The **Reset to Factory Default** page allows you to reset the ADSL Bridge/Router to original factory default configuration.

Diagnostic Test

The **Diagnostic Test** page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides. This page will continually refresh every 2 seconds until all tests are complete.



Testing Ethernet LAN Connection: This test passes if the Ethernet LAN interface is working properly.

Testing ADSL Synchronization: This test checks your ADSL Bridge/Router to see if it can successfully negotiate and establish an ADSL connection with your service provider. The test returns PASS if an ADSL connection is established. If this test returns FAIL, please try the test again a few minutes after this test is completed. Your ADSL bridge/Router needs up to one minute to establish the ADSL connection depending on your phone line quality. If this test returns FAIL, make sure your phone line is connected to your ADSL Bridge/Router secured, and also check with your service provider to see if your service is activated. If this test returns FAIL, all other tests will be skipped.

Test ATM OAM Segment Loop Back: This test sends ATM OAM F5 Segment loop back request cells to the CO. This test will pass if a response cell is received. Since some service providers might not support this test, it could still work even if this test fails. If this test fails consistently and the ADSL Bridge/Router seems not working, make sure the VPI and VCI are configured correctly. This test returns FAIL if the ADSL synchronization test failed.

Test ATM OAM End-to-End Loop Back: This test sends ATM OAM F5 End to End loop back request cells to the central office equipment through your ADSL connection. This test returns PASS if response cell is received. Since your service provider might not support this test, your ADSL Bridge/Router could still be working properly even if this test fails. If this test returns FAIL consistently and your ADSL Bridge/Router seems to not be working, check to make sure the VPI and VCI are configured correctly. This test returns SKIPPED if the ADSL synchronization test failed.

Test Ethernet Connect to ATM: This test returns PASS if the ATM AAL5 module is loaded correctly in your ADSL Bridge/Router. If this test returns FAIL, an internal error has occurred. This test returns SKIPPED if the ADSL synchronization does not return PASS.

Test PPPoE Connection: This test returns PASS if your ADSL Bridge/Router can see the PPPoE server. If this test returns FAIL, run this test again a few minutes after this test is completed, especially if your PPPOE connection has just been improperly disconnected. If this test consistently returns FAIL, make sure that the PPPoE settings are in the correct configuration as instructed by your service provider, make sure the VPI and the VCI settings of the current VC are configured correctly. This test returns SKIPPED if the "AAL5 Connection" test does not return PASS.

Test PPP Layer Connection: This test returns PASS if your login name and password have passed authentication with your service provider. If this test returns FAIL, run this test again a few minutes after this test is completed, especially if your PPP connection has just been improperly disconnected. If this test consistently fails, first make sure your login name and password are correct. Remember that login names and psswords are case sensitive.

This test returns SKIPPED if the "PPPoE Connection" test does not return PASS and your ADSL modem is configured as PPPoE encapsulation. This test also returns SKIPPED if the "AAL5 Connection" test does not return PASS and your ADSL Bridge/Router is configured for PPPOA encapsulation.

Test IP Connect to PPP: This test returns PASS if your ADSL Bridge/Router has been assigned a valid IP address by your service provider through DHCP or your ADSL Bridge/Router is assigned a valid IP address statically. If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Bridge/Router is statically assigned an IP address, make sure the IP address is the correct one assigned by your service provider. This test returns SKIPPED if the "AAL5 Connection" test does not return PASS.

Ping Gateway: This test returns PASS if the gateway can be reached through a ping request. The gateway is assigned by your service provider, or obtained from your service provider by PPP or DHCP negotiation. If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Bridge/Router seems not working, check to make sure your statically assigned IP address is configured correctly or the DHCP client is enabled on with the current VC. This test returns SKIPPED if the "IP Assignment" test does not return PASS.

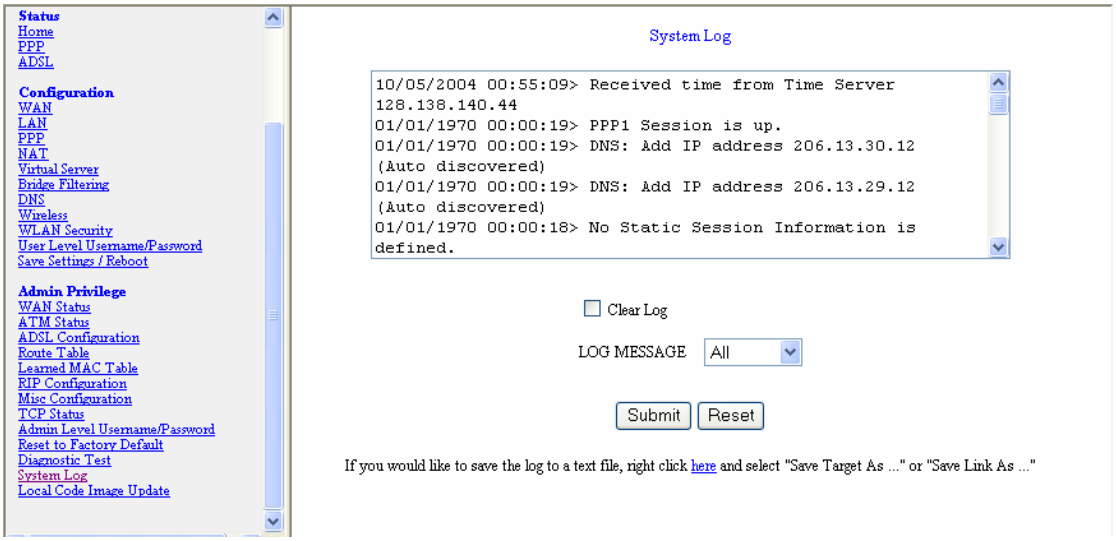
Ping Primary DNS: This test returns PASS if the primary DNS can be reached through a ping request. The primary DNS is assigned by your service provider or obtained from your service provider by PPP or DHCP negotiation. If this test returns FAIL, run this test again a few minutes after this test is completed. If this test returns FAIL consistently and your ADSL Bridge/Router seems to not be working, check to make sure your statically assigned primary DNS IP address is configured correctly or DHCP client is enabled with the current VC. This test returns N/A if there is no DNS configured.

Query DNS for www.conexant.com: This test returns PASS if the host name can be resolved to an IP address though your domain name servers. This test returns FAIL if the host name can not be resolved successfully. If this test returns FAIL, run this test again a few minutes after this test is completed.

Ping www.conexant.com: This test returns PASS if the host specified by your ISP can be reached through a ping request. If this test returns FAIL, run this test again a few minutes after this test is completed. This test returns SKIPPED if the host name can not be resolved to an IP address.

System Log

The **System Log** page shows the events triggered by the system. This page contains information that is dynamic and will refresh every 5 seconds.



Clear Log: This field allows you to clear the current contents of the System Log.
Save Log: This field allows you to save the current contents of the System Log by right click HERE and select “Save Target As” to save it into a text file.

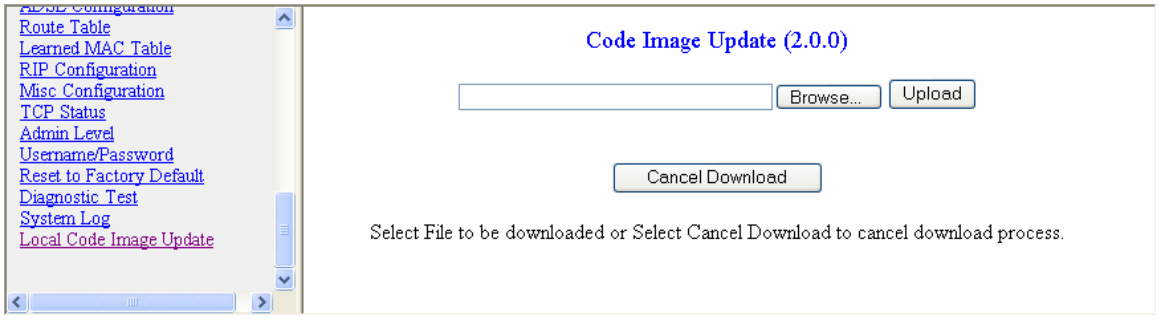
The **System Log** records:

- **ADSL Layer**
  - ADSL Link detected
  - ADSL Link connected
  - ADSL Link disconnected
- **ATM Layer**
  - ATM detected
  - ATM connected
  - ATM disconnected
  - ATM setting up VPI/VCI

- **PPP Layer**
  - PPP authenticated
  - PPP invalid user name or password
  - PPP unable to connect with PPP server
- **IP Layer**
  - IP protocol up
  - PPP IP address
  - PPP Gateway IP address PPP DNS Primary IP address
  - PPP DSN Secondary IP address

Local Code Image Update

The **Code Image Update** page allows you to upgrade the image code locally.

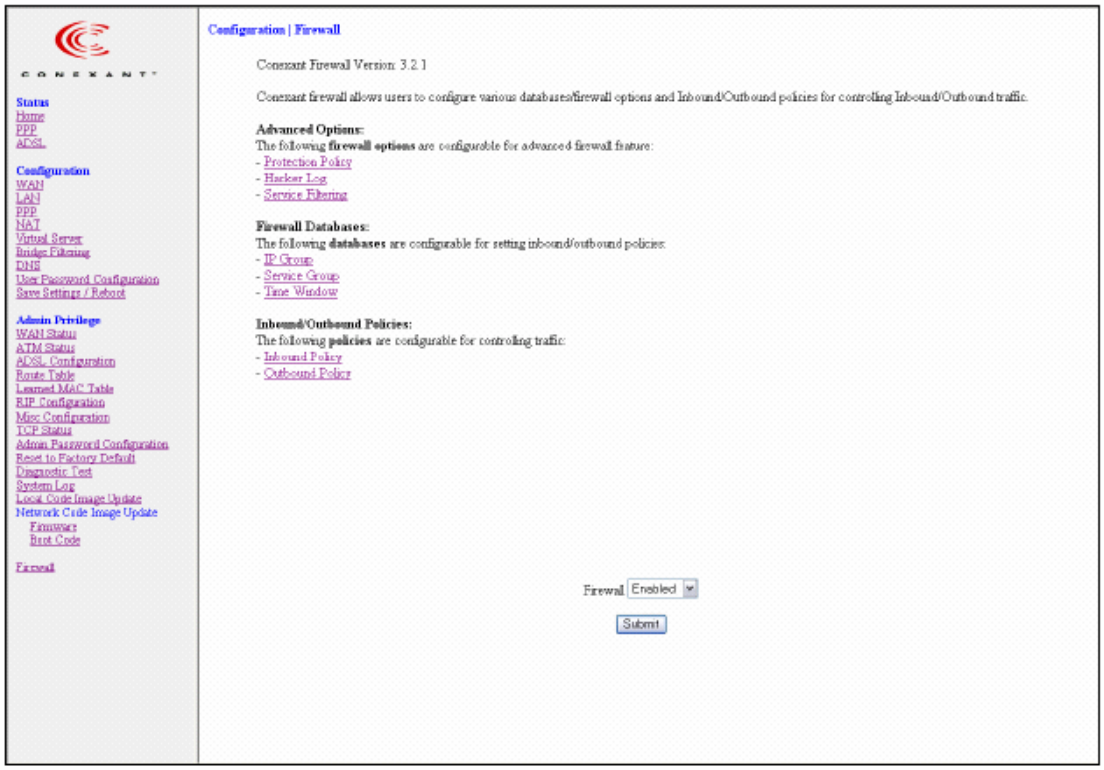


Browse the location of file, firmware.dlf or bootrom.dlf file, and click the Upload to start the update. The ADSL Bridge/Router will reboot as part of the process of updating code.

CHAPTER 8 FIREWALL CONFIGURATION

A Statefull Packet Inspection (SPI) firewall is an optional feature that may or may not be included in your ADSL Bridge/Router.

A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.



Advanced Options: This section contains options for protecting against particular wellknown attacks as well as documenting those attacks as they occur.

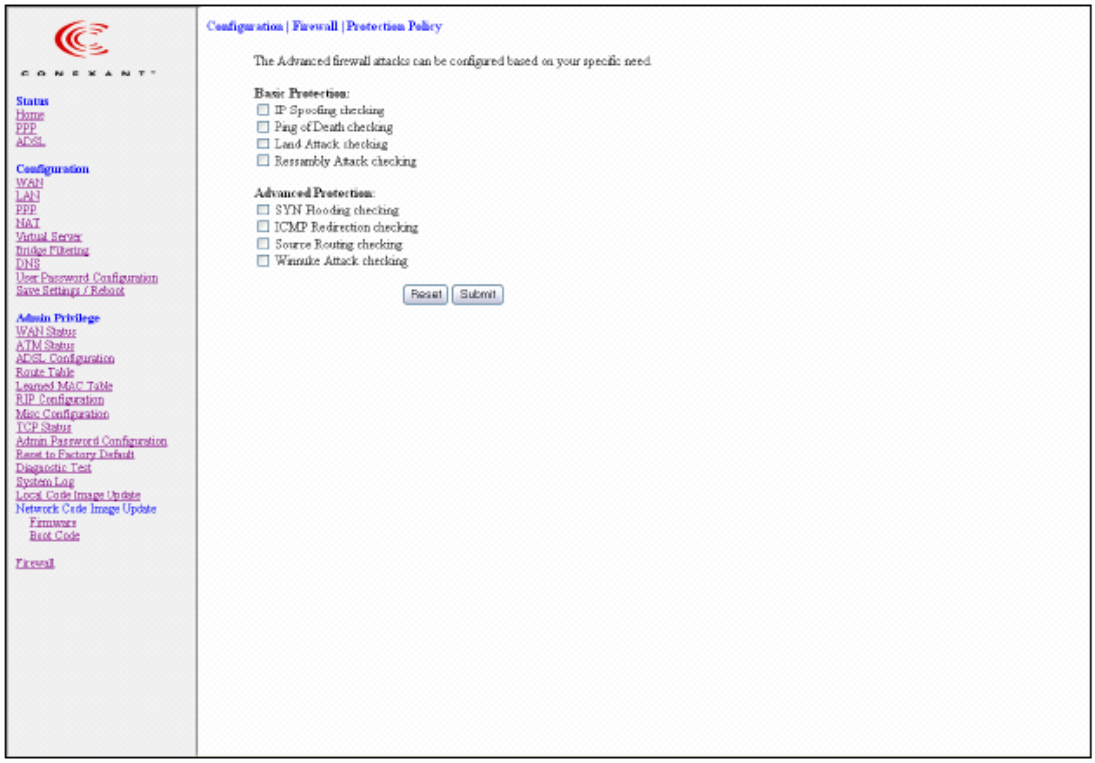
Firewall Databases: This section allows you to create groups based on IP addresses, subnet masks, ports, and time. These groups are used when creating inbound and outbound policies.

Inbound/Outbound Policies: This section allows you to create rules for incoming and outgoing IP packets. The IP packets are compared against the rules and are allowed or denied accordingly.

Firewall Enable/Disable: This option enables/disables all the protection provided on these pages.

Protection Policy

Protection Policies defend against common methods of attacking a network and computers within the network. Some of these attacks are classified as a DoS (Denial of Service). DoS is an attack in which a network or components of a network are disabled, usually by overloading traffic on the network, in order to prevent authorized and legitimate users to access network resources.



Basic Protection:

- **IP Spoofing checking:** IP spoofing is when an unauthorized user inserts the IP address of an authorized user into the IP packets in order to gain access to a network. Selecting this option will allow the firewall to check for and filter out this discrepancy.

- **Ping of Death checking:** Ping of Death is a type of DoS attack that uses a malformed ICMP data packet that contains unusually large amounts of data that causes TCP/IP to crash or behave irregularly. Enabling this will allow the firewall to filter out packets containing Ping of Death properties.

• **Land Attack checking:** Land attack is a type of DoS attack that works by sending a spoofed packet containing the same source and destination IP address and port (the victim's IP address). This packet contains a connection request, resulting in a handshake process. At the end of the handshake, the victim sends out an ACK (ACKnowledge) request. Since the source and the destination are the same, the victim receives the ACK request it just sent out. The received data does not match what the victim is expecting, so it retransmits the ACK request. This process repeats until the network crashes. Enabling this will allow the firewall to filter out possible Land Attack packets.

• **Reassembly Attack checking:** Reassembly Attack is a type of DoS attack that exploits the weakness of the IP protocol reassembly process. As discussed earlier in this user guide, packets undergo fragmentation when they exceed a certain maximum size. Certain criteria define the packet fragmentation process so that packets can be reassembled properly. In Reassembly Attack, the subpackets have malformed criteria (fragment offset), which can easily cause a system to crash, freeze, or reboot. Enable this option to check for and filter out Reassembly Attack packets.

Advanced Protection:

• **SYN Flooding checking:** SYN Flooding is a type of DoS attack that is accomplished by not sending the final acknowledgement to the receiving server's SYN-ACK (SYNchronize-ACKnowledge) in the final part of the handshake process. This causes the serve to keep signaling until it is timed out. When a flood (many) of these attacks are sent simultaneously, the server will probably overload and crash. Enable SYN Flooding checking to filter out possible SYN flood packets.

• **ICMP Redirection checking:** Also known as an ICMP storm attack or smurf attack, ICMP Redirection is another form of DoS. This attack is performed by sending ICMP echo requests to a broadcast network node. The return IP address is spoofed and replaced by the victim's own address, causing it to send the request back to itself. This causes the broadcast address to send it out to all the network nodes in the broadcast area (usually the entire LAN). In turn, all those recipients resend it back to the broadcast. The process repeats itself, gaining more amplitude through each iteration and eventually causing a traffic overload and crashing the network. Enable ICMP Redirection checking to filter out packets containing the threat.

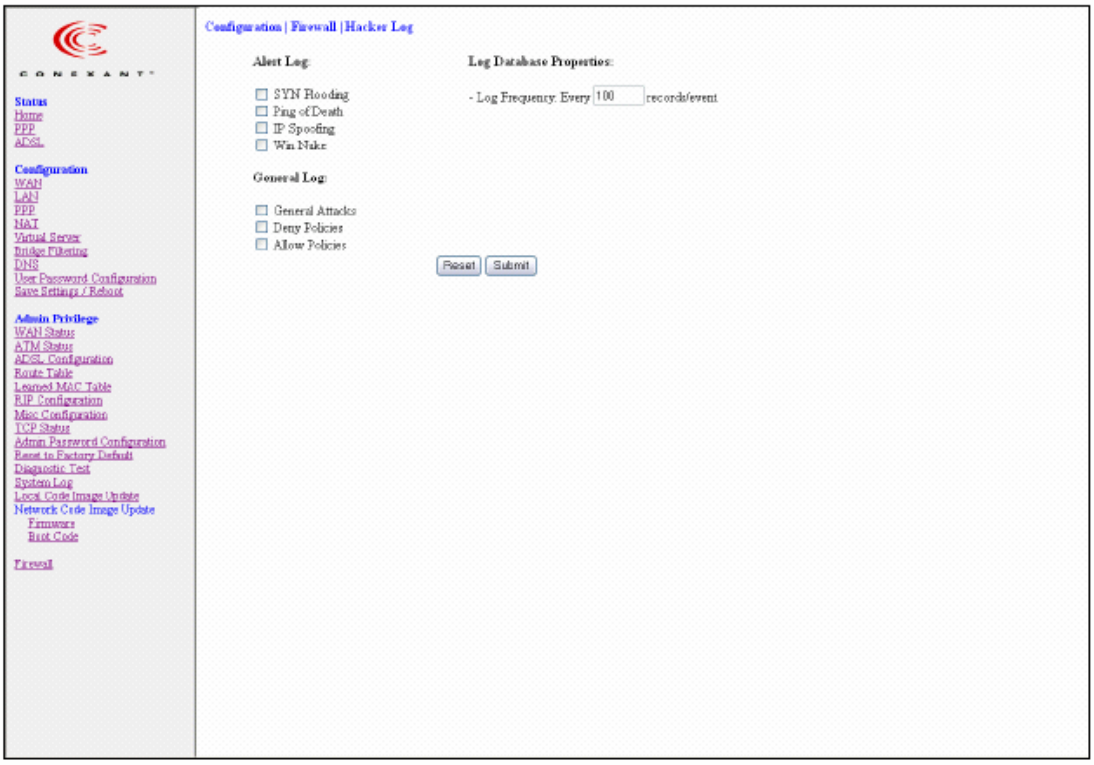
• **Source Routing checking:** Source routing gives the sender of a packet the ability to determine the exact route that an IP packet takes to get to the destination. However, source routing can be used for malicious reasons. Using a source routed packet, the sender could find out important information about

nodes in a network, making it easy to exploit any weakness. Enabling Source Routing checking will cause the firewall to filter out any packet with Source Routing properties.

• **WinNuke Attack checking:** WinNuke exploits a large networking bug found in Windows 95 and NT. WinNuke sends erroneous OOB (Out-of-Band) data that Windows is unable to process, causing the target computer to crash. Enable this if you are running an early (95 or NT) version of Windows that is vulnerable to this attack.

Hacker Log

This page allows you to configure which Protection Policy (see previous section) violations to log for admin viewing.



Alert Log: Enable/Disable for SYN Flooding, Ping of Death, IP Spoofing, and Win Nuke (all of these are explained in the previous section). Enable to log violations of individual policies.

General Log:

• Deny Policies: Enabling this will add Deny Policy violations to the log. Deny Policies are discussed later in the Inbound/Outbound policy section.

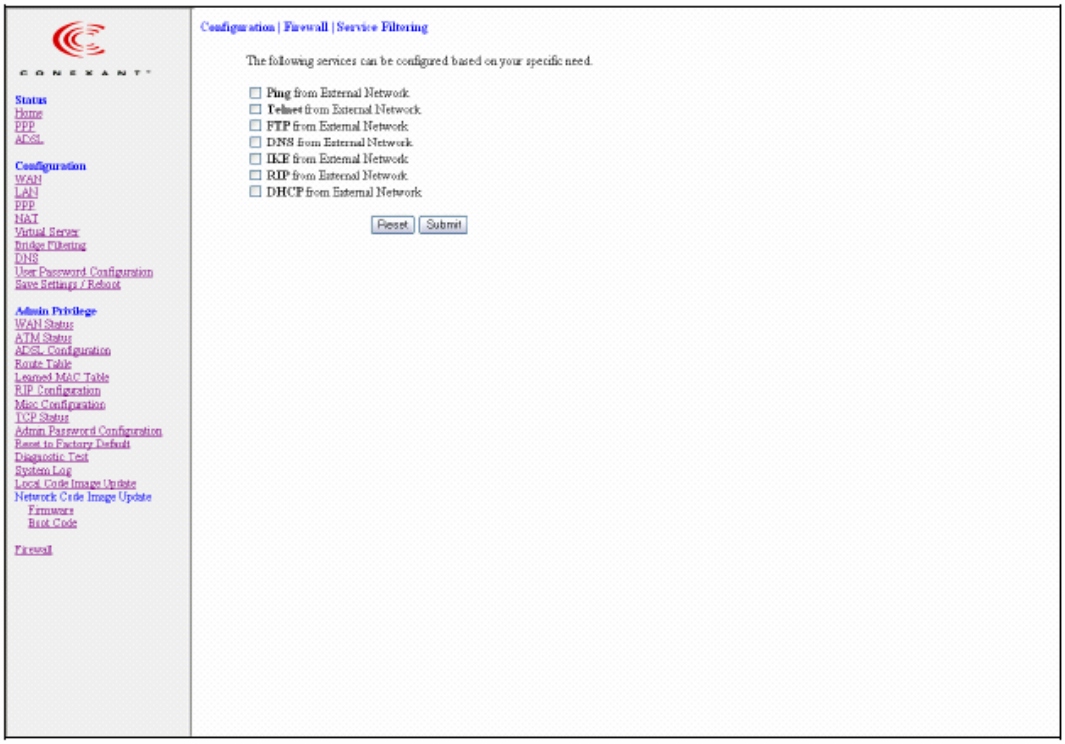
• Allow Policies: Enabling this will add Allow Policy acceptances to the log. Allow Policies are discussed later in the Inbound/Outbound policy section.

Log Database Properties:

• Log Frequency: This field lets you specify how many records to keep of each event. Default is 100. Range for Log Frequency Field is 1-65535.

Service Filtering

Service Filtering allows you to disable service requests from certain sources.



These are the Service Request sources that can be disabled:

- **Ping from External Network**
- **Telnet from External Network**
- **FTP from External Network**
- **DNS from External Network**
- **IKE from External Network**
- **RIP from External Network**
- **DHCP from External Network**

IP Group

The IP Group lets you specify IP Addresses (Single or Range) and Subnet Masks and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

IP Entry Name: This is the name you assign to the group of IP addresses and subnet masks.

The IP Entry Name can be up to 19 characters.

IP addr. 1: This is the IP address or subnet mask you are specifying when creating a group.

IP addr. 2: This field is only active if you select to group a range of IP ddresses or subnet masks, in which case this is the end address of that range whereas the IP addr 1 is the first address of that range.

IP/Mask: This field allows you to specify the address type assigned to the group.

- Single IP: This will let you specify one IP address for a given group.
- IP Range: This will let you specify a range of IP addresses for a given group, starting with IP addr 1 and ending with IP addr 2.
- Subnet Mask: This will let you specify a range of subnet masks for a given group.

Service Group

The Service Group lets you specify a Port and assign it to a group name for easy use when configuring inbound and outbound policies for the firewall.

Service Entry Name: This is the name you assign to the group containing the port number.

The Service Name Entry can be up to 19 characters.

TCP/UDP: This specifies whether the port goes through TCP or UDP.

Port #: This is the port number associated with the group name.
Range for Port # is 1 – 65535.

Time Window

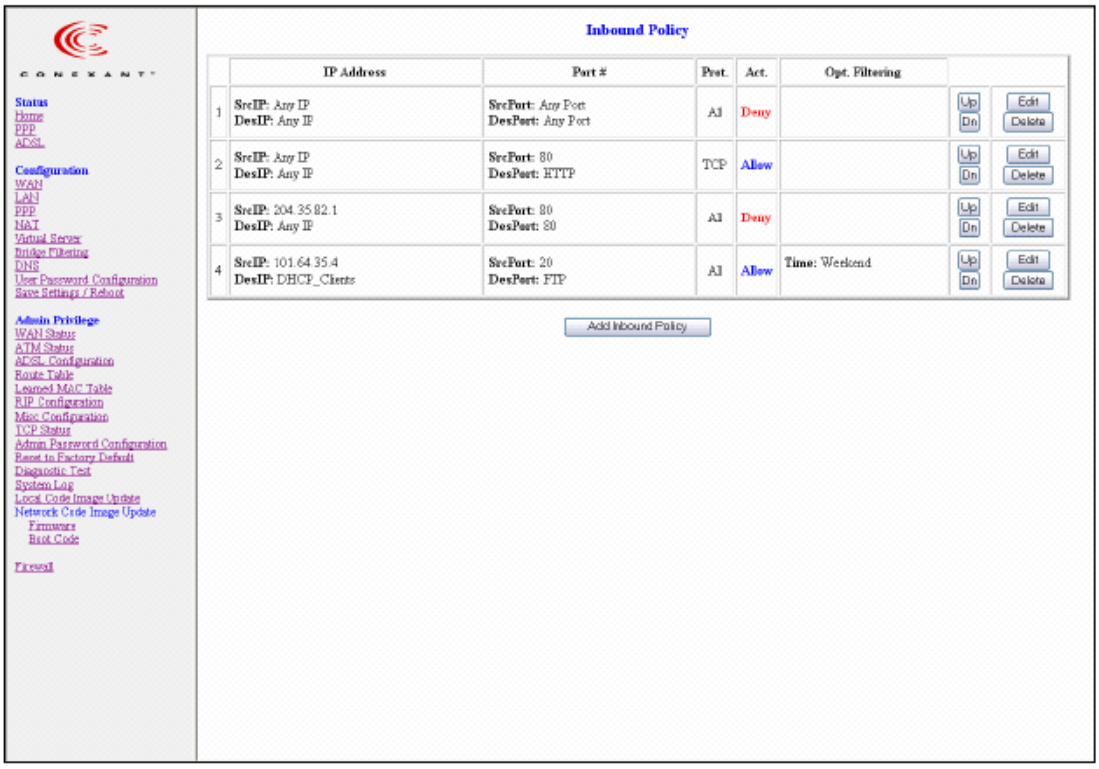
The Time Window lets you specify certain time periods and assign them to a group name for easy use when configuring inbound and outbound policies for the firewall.

Time Window Name: This is the name you assign to the group that is given the time designation. The Time Window Name can be up to 19 characters.

Time Period: This field allows you to specify the time period for both start time and end time by selecting the day, hour, minute, and AM/PM.

Inbound Policy

The Inbound Policy allows you to filter inbound (from the WAN into the user side LAN) packets based on a set of rules. This enables you to deny access from different sources and thus increase security.



A table of inbound policies is displayed with the following information. If there are no policies, then a message stating "*No Entries in Inbound Policy Database*" will be displayed in place of the table.

IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act.: Short for action, this field specifies two possible actions: allow or deny.

Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.

Up: Clicking this button will move the corresponding policy up one space in the table.

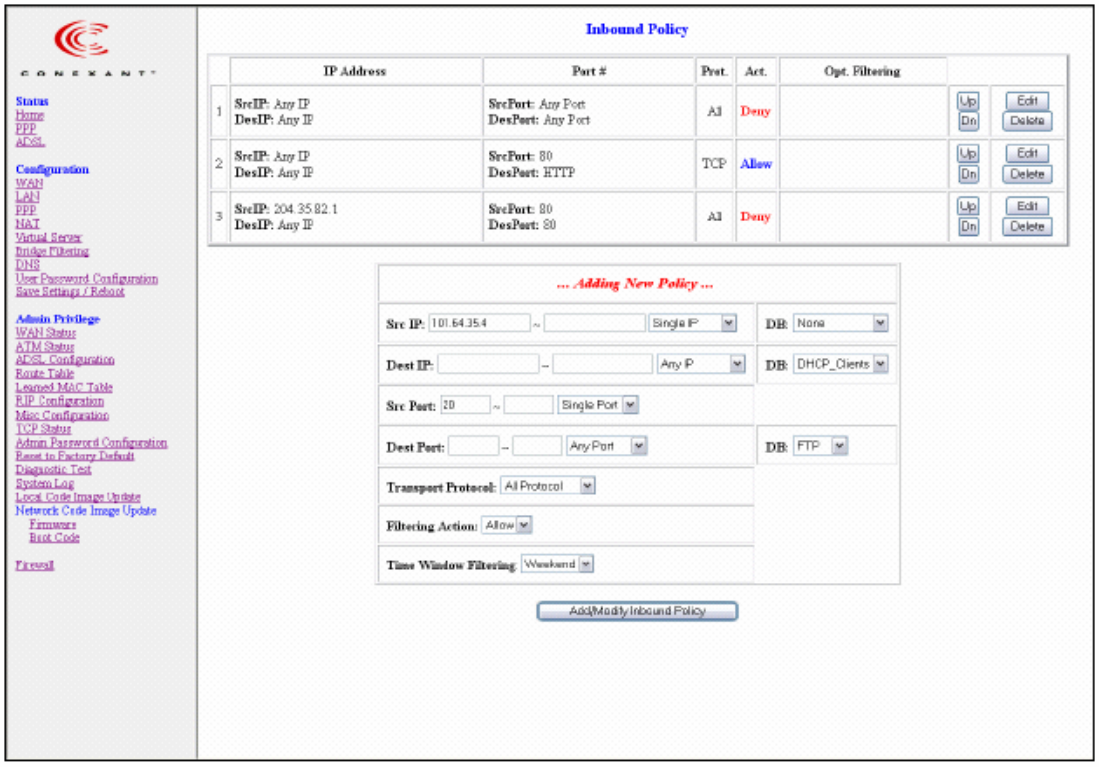
Dn: Short for down, clicking this button will move the corresponding policy down one space in the table.

Note: The Inbound Policy works in a Top-Down fashion according to the Inbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have inbound policies in the correct order. See Section 6.9.1 for an example of this.

Edit: Clicking this button will display a table similar to the add table (see below) to the bottom of the policy table that will allow you to modify the corresponding policy.

Delete: This will delete the corresponding policy.

Add Inbound Policy: Clicking this button will bring up a table with all the add configurations as shown below:



Src IP: This specifies the Source IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and Subnet Masks that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:

- **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

- **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must beentered into the second IP Address entry field.

- **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. See **Src IP** above for configuration detail.

Src Port: This specifies the Source Port for the Inbound Policy. This is the external (WAN side, outside of the firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

- **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

- **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

• **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

• **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (LAN side, behind the firewall) Port that will be affected by the policy. See **Src Port** above for configuration detail.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

Filtering Action: This specifies what action the policy takes:

• **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

• **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All ofthese are specified above and must be configured by the user.

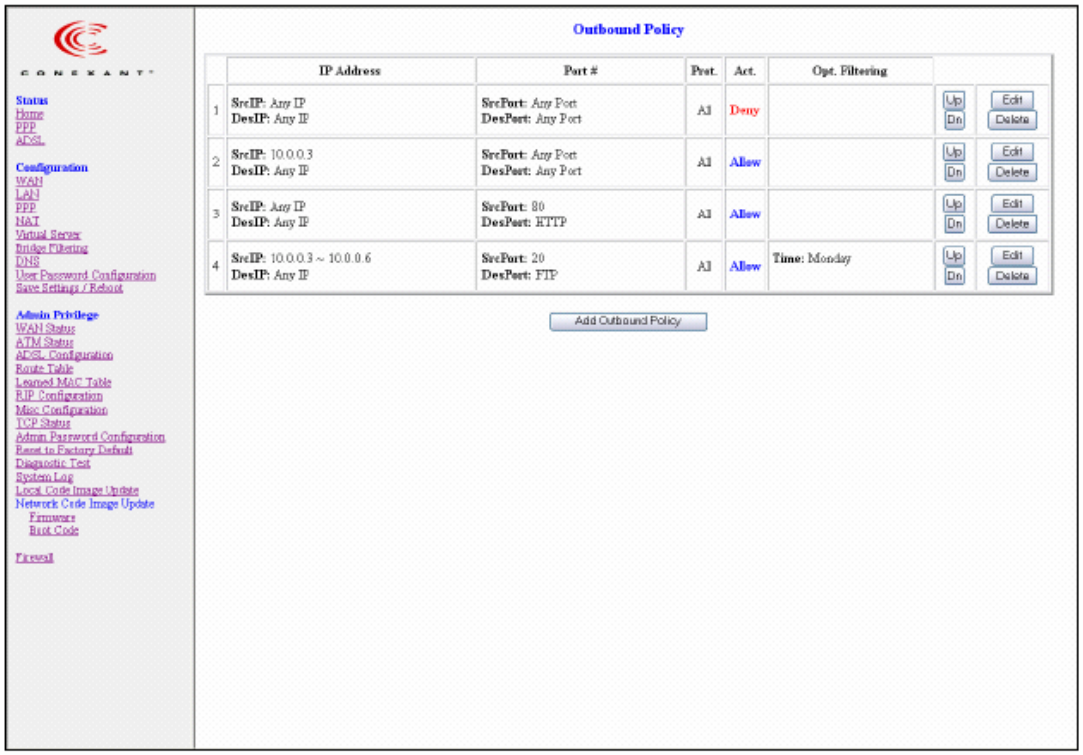
Time Window Filtering: This field allows you to select a certain time frame from the **Time Group** in which this policy will be active. See section 6.6 for more information on Time Groups.

DB: Short for Database, this field allows you to select a user-defined IP Group for the **Src IP** and **Dest IP** fields and a user-defined Service Group for the **Dest Port**. Userdefined IP and Service Groups are created in **IP Group** and **Service Group** pages, sections 6.4 and 6.5, respectively, in this user guide.

Note: Source and Destination IP Addresses, Subnet Masks, and Ports are reversed between Inbound Policy and Outbound Policy. For Inbound Policy, the source is on the WAN side and the destination is on the LAN side. For Outbound policy, the source is on the LAN side and the destination is on the LAN side.

Outbound Policy

The Outbound Policy allows you to filter outbound (from the user side LAN to the WAN) packets based on a set of rules. This enables you to deny access to different sources and thus increase security.



A table of outbound policies is displayed with the following information. If there are no policies, then a message stating “No Entries in Outbound Policy Database” will be displayed in place of the table.

IP Address: This field specifies the IP address or addresses to which the policy applies. Both the source IP (SrcIP) and destination IP (DesIP) are specified here.

Port #: This field specifies the Port number to which the policy applies. Both the source port (SrcPort) and destination port (DesPort) are specified here.

Prot.: Short for protocol, this is the protocol to which the policy applies.

Act. Short for action, this field specifies two possible actions: allow and deny.

Opt. Filtering: Optional Filtering field specifies the time period to which the policy applies.

Up: Clicking on this button will move the corresponding policy up one space in the table.

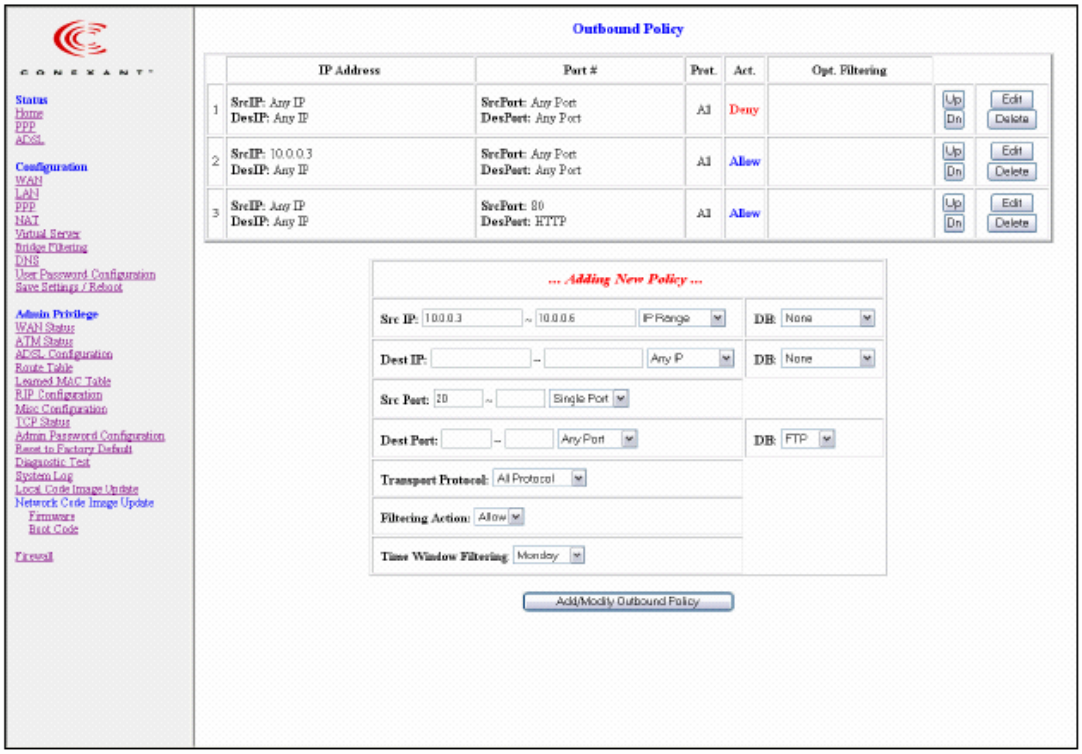
Dn: Short for down, clicking on this button will move the corresponding policy down one space in the table.

Note: The Outbound Policy works in a Top-Down fashion according to the Outbound Policy Table. This means that the firewall will apply the policies in order from the top of the table to the bottom. It is critical for both security and user accessibility to the WAN to have outbound policies in the correct order. See Section 6.9.1 for an example of this.

Edit: Clicking this button will display a table similar to the add table (see next page) to the bottom of the policy table that will allow you to modify the corresponding policy.

Delete: This will delete the corresponding policy.

Add Inbound Policy: Clicking on this button will bring up a table with all the add configurations as shown below:



Src IP: This specifies the Source IP for the Outbound Policy. This is the internal (LAN side, behind the firewall) IP address or addresses and Subnet Mask(s) that will be affected by the policy. In this field there are two IP Address entry fields and a dropdown menu. The dropdown menu has four options:

- **Any IP**: Selecting this will cause all IPs to be affected by the policy. When this is selected, you will be unable to enter any information into the IP Address entry fields.

- **Single IP**: Selecting this will cause only one IP Address to be affected by the policy. This IP Address will need to be specified by the user in the first IP Address entry field.

- **IP Range**: Selecting this will enable you to select a range of IP Addresses to which the policy will apply. The first IP Address in the range must be entered into the first IP Address entry field and the last IP Address in the range must be entered into the second IP Address entry field.

- **Mask Range:** Selecting this will enable you to select a range of Subnet Masks to which the policy will apply. The first Subnet Mask in the range must be entered into the first IP Address entry field and the last Subnet Mask in the range must be entered into the second IP Address entry field.

Dest IP: This specifies the Destination IP for the Inbound Policy. This is the external (WAN side, outside of the firewall) IP address or addresses and subnet mask(s) that will be affected by the policy. See **Src IP** above for configuration detail.

Src Port: This specifies the Source Port for the Inbound Policy. This is the internal (LAN side, behind firewall) port(s) that will be affected by the policy. In this field, there are two port entry fields and a dropdown menu. The dropdown menu has four options:

- **Any Port:** Selecting this will cause all Ports to be affected by the policy. When this is selected, you will be unable to enter any information into the Port entry fields.

- **Single Port:** Selecting this will cause only one Port to be affected by the policy. This Port will need to be specified by the user in the first Port entry field.

- **Port Range:** Selecting this will enable you to select a range of Ports to which the policy will apply. The first Port in the range must be entered in the first Port entry field and the last Port in the range must be entered in the second Port entry field.

• **Safe Ports:** Any port greater than 1024 (1025 – 65535) is considered a safe port.

Dest Port: This specifies the Destination Port for the Inbound Policy. This is the internal (WAN side, outside of the firewall) Port that will be affected by the policy. See **Src Port** above for configuration detail.

Transport Protocol: This specifies the Transport/Transfer protocol for the policy. The following protocol options are available: All, TCP, UDP, ICMP, AH, ESP, and GRE.

Filtering Action: This specifies what action the policy takes:

• **Allow:** Selecting this will cause the policy to allow packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

• **Deny:** Selecting this will cause the policy to deny packet transfer from the **Src IP** through the **Src Port** to travel through the **Dest Port** to the **Dest IP**. All of these are specified above and must be configured by the user.

Time Window Filtering: This field allows you to select a certain time frame from the **Time Group** in which this policy will be active. See section 6.6 for more information on Time Groups.

DB: Short for Database, this field allows you to select a user-defined IP Group for the **Src IP** and **Dest IP** fields and a user-defined Service Group for the **Dest Port**. Userdefined IP and Service Groups are created in **IP Group** and **Service Group** pages, sections 6.4 and 6.5, respectively..

Inbound/Outbound Policy Sample Configuration

This is a sample Inbound/Outbound configuration meant to guide you in making your own configurations. This configuration does not necessarily provide proper security, it is meant only as a sample to display the functionality of the Inbound and Outbound Policies.

Inbound Policy

Sample Configuration: You want your firewall to have the following properties:

• Accept all http IP addresses, except for 204.35.82.1

• Grant FTP access from 101.64.35.4 (external) to 10.0.0.3, 10.0.0.4, 10.0.0.5, and 10.0.0.6 (all internal).

• Deny all access to FTP Server 10.0.0.6 on the weekend. Converting the access requirements from above so that the Inbound Policy can understand them yields the following:

• Deny access from any Src (WAN) IP to any Des (LAN) IP through any source or destination port and through all protocols.

• Allow access from any Src (WAN) IP to any Des (LAN) IP through port 80 (HTTP), through TCP.

• Deny access from Src (WAN) IP 204.35.82.1 to any Des (LAN) IP through port 80 (HTTP), through TCP.

• Allow access from Src (WAN) IP 101.64.35.4 to Des (LAN) IP 10.0.0.3 ~ 10.0.0.6 through port 20 (FTP), through TCP.

• Deny access from any Src (WAN) IP to **DB** FTP (defined as) IP through any source or destination protocol and through all protocols during time period WEEKEND, where WEEKEND is defined in the **Time Group** as Saturday, 12:00AM to Sunday, 11:59PM.

It does not matter which order you input these in as long as you sort them into the correct order once you are finished.

The configuration should look like the following when complete:

	IP Address	Port #	Prot.	Act.	Opt. Filtering		
1	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** Any Port **DesPort:** Any Port	All	Deny		Up Dn	Edit Delete
2	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** 80 **DesPort:** 80	TCP	Allow		Up Dn	Edit Delete
3	**SrcIP:** 204.35.82.1 **DesIP:** Any IP	**SrcPort:** 80 **DesPort:** 80	TCP	Deny		Up Dn	Edit Delete
4	**SrcIP:** 101.64.35.4 **DesIP:** 10.0.0.3 ~ 10.0.0.16	**SrcPort:** 20 **DesPort:** 20	TCP	Allow		Up Dn	Edit Delete
5	**SrcIP:** Any IP **DesIP:** FTP_Server	**SrcPort:** 20 **DesPort:** 20	All	Deny	**Time:** WEEKEND	Up Dn	Edit Delete

Note: It should be clear now how critical it is to sort the policies in the correct order. For example, if policies one and two were switched, there would be NO HTTP access to any computer in the LAN. This would make web browsing impossible.

Outbound Policy

Sample Configuration: You want to deny all access to the WAN except for the following:

- HTTP access from any IP through TCP.
- Any access from 10.0.0.3 through any protocol.
- FTP Access from 10.0.0.3~10.0.0.6 through any protocol

Converting the access requirements from above so that the Outbound Policy can understand them yields the following:

- Deny all access from any Src (LAN) IP to any Des (WAN) IP through any source or destination port and through any protocol.
- Allow access from Src (LAN) IP 10.0.0.3 to any Des (WAN) IP through any port through any protocol.
- Allow access from any Src (LAN) IP to any Des (WAN) IP through port 80(HTTP), through TCP.

• Allow access from Src (LAN) IP range 10.0.0.3~10.0.0.6 to any Des (WAN) IP through port 20 (FTP), through any protocol.

The configuration should look like the following when complete:

	IP Address	Port #	Prot.	Act.	Opt. Filtering		
1	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** Any Port **DesPort:** Any Port	All	Deny		Up Dn	Edit Delete
2	**SrcIP:** 10.0.0.3 **DesIP:** Any IP	**SrcPort:** Any Port **DesPort:** Any Port	All	Allow		Up Dn	Edit Delete
3	**SrcIP:** Any IP **DesIP:** Any IP	**SrcPort:** 80 **DesPort:** HTTP	All	Allow		Up Dn	Edit Delete
4	**SrcIP:** 10.0.0.3 ~ 10.0.0.16 **DesIP:** Any IP	**SrcPort:** 20 **DesPort:** FTP	All	Allow		Up Dn	Edit Delete

Appendix A: ADSL ETHERNET MODEM ROUTER CONFIGURATION

Bridge Mode Configuration

WAN Configuration	
Default Gateway	0.0.0.0
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Encapsulation	1483 Bridged IP LLC
Bridged	Enabled
IGMP	Disabled
PPP Service Name	N/A
PPP User Name	N/A
PPP password	N/A
DHCP Client	Disabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0
DHCP server	Disabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0
User mode	Multi-user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	Disabled
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers only
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
ADSL Configuration	
Trellis	Enabled
Handshake protocol	Autosense-G.dmt first
Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False

Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Disabled

Router Mode Configuration with Dynamic IP

WAN Configuration	
Default Gateway	0.0.0.0
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Encapsulation	1483 Bridged IP LLC
Bridged	Disabled
IGMP	Disabled
PPP Service Name	N/A
PPP User Name	N/A
PPP password	N/A
DHCP Client	Enabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0
DHCP server	Enabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0
User mode	Multi-user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	NAPT
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers only
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
ADSL Configuration	
Trellis	Enabled

Handshake protocol	Autosense-G.dmt first

Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False
Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Disabled

Router Mode Configuration with Static IP

WAN Configuration	
Default Gateway	Provided by ISP
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	Provided by ISP
Subnet Mask	Provided by ISP
Encapsulation	1483 Bridged IP LLC
Bridged	Disabled
IGMP	Disabled
PPP Service Name	N/A
PPP User Name	N/A
PPP password	N/A
DHCP Client	Disabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0
DHCP server	Enabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0
User mode	Multi-user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	NAPT
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers

	only
Preferred DNS Server	Provided by ISP
Alternate DNS Server	Provided by ISP
ADSL Configuration	
Trellis	Enabled
Handshake protocol	Autosense-G.dmt first
Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False
Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Disabled

Router Mode PPPoA Configuration (RFC2364)

WAN Configuration	
Default Gateway	0.0.0.0
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Encapsulation	PPPoA VC-Mux
Bridged	Disabled
IGMP	Disabled
PPP Service Name	N/A (Required by some ISPs)
PPP User Name	Provided by ISP
PPP password	Provided by ISP
DHCP Client	Disabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0
DHCP server	Enabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0

User mode	Multi-user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	NAPT
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers only
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
ADSL Configuration	
Trellis	Enabled
Handshake protocol	Autosense-G.dmt first
Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False
Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Enabled

Router Mode PPPoE Configuration (RFC2516)

WAN Configuration	
Default Gateway	0.0.0.0
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Encapsulation	PPPoE LLC
Bridged	Disabled
IGMP	Disabled
PPP Service Name	N/A (Required by some ISPs)
PPP User Name	Provided by ISP
PPP password	Provided by ISP
DHCP Client	Disabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0

DHCP server	Enabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0
User mode	Multi-user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	NAPT
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers only
Preferred DNS Server	0.0.0.0
Alternate DNS Server	0.0.0.0
ADSL Configuration	
Trellis	Enabled
Handshake protocol	Autosense-G.dmt first
Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False
Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Enabled

Router Mode Configuration with Classical IP over ATM (RFC1577)

WAN Configuration	
Default Gateway	Provided by ISP
VC Setting	Enabled
VPI	Provided By ISP
VCI	Provided By ISP
Static IP Address	Provided by ISP
Subnet Mask	Provided by ISP
Encapsulation	Classical IP over ATM
Bridged	Disabled
IGMP	Disabled
PPP Service Name	N/A
PPP User Name	N/A

PPP password	N/A
DHCP Client	Disabled
Host name	N/A
Virtual Circuit	0
LAN Configuration	
LAN IP	10.0.0.2
LAN subnet mask	255.0.0.0
DHCP server	Enabled
DHCP address pool selection	User Defined
User defined start address	10.0.0.3
User defined end address	10.0.0.14
Lease Time	0
User mode	Single user
Ethernet mode	Autosense
NAT Configuration	
NAT Configuration	NAPT
DNS Configuration	
DNS proxy selection	Use auto discovered DNS servers only
Preferred DNS Server	Provided by ISP
Alternate DNS Server	Provided by ISP
ADSL Configuration	
Trellis	Enabled
Handshake protocol	Autosense-G.dmt first
Wiring Selection	Tip/Ring
RIP Configuration	
RIP	Disabled
Supplier	True
Gateway	False
Multicast	False
Interval	30 seconds
Misc Configuration	
WAN side HTTP server	Disabled
FTP server	Disabled
TFTP server	Disabled
HTTP server port	80
DMZ	Disabled
DMZ Host IP	0.0.0.0
DNS Proxy	Enabled
DHCP Relay	Disabled
IGMP proxy	Disabled
PPP reconnect on WAN access	Disabled